99TH CONGRESS
2d Session

SENATE

REPORT
99-522

MEETING THE ESPIONAGE CHALLENGE: A REVIEW OF UNITED STATES COUNTERINTELLIGENCE AND SECURITY PROGRAMS

REPORT

OF THE

SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE

OCTOBER 3 (legislative day, SEPTEMBER 23), 1986.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE

64-268 O

WASHINGTON : 1986

S423-2

SENATE SELECT COMMITTEE ON INTELLIGENCE

[Established by S. Res. 400, 94th Cong., 2d Sess.]

DAVE DURENBERGER, Minnesota, *Chairman*
PATRICK J. LEAHY, Vermont, *Vice Chairman*

WILLIAM V. ROTH, JR., Delaware
WILLIAM S. COHEN, Maine
ORRIN HATCH, Utah
FRANK MURKOWSKI, Alaska
ARLEN SPECTER, Pennsylvania
CHIC HECHT, Nevada
MITCH McCONNELL, Kentucky

LLOYD BENTSEN, Texas
SAM NUNN, Georgia
THOMAS F. EAGLETON, Missouri
ERNEST F. HOLLINGS, South Carolina
DAVID L. BOREN, Oklahoma
BILL BRADLEY, New Jersey

ROBERT DOLE, Kansas, *Ex Officio*
ROBERT C. BYRD, West Virginia, *Ex Officio*

BERNARD F. MCMAHON, *Staff Director*
ERIC D. NEWSOM, *Minority Staff Director*
DORTHEA ROBERTSON, *Clerk*

CONTENTS

	Page
I. Introduction and Summary	1
A. Background	1
B. Organization of the U.S. Government to Meet the Hostile Intelligence Challenge	3
C. Counterintelligence: Learning the Lessons of Recent Cases	4
D. Security Countermeasures: Defending on Many Fronts	6
E. Budgetary Impact	9
F. Legislative Proposals	10
G. Respect for Individual Rights	11
II. The Hostile Intelligence Threat	12
A. Damage to National Security	12
B. Sources of the Threat	17
1. Soviet Union	17
2. Warsaw Pact and Cuba	18
3. People's Republic of China	19
4. Other Countries	20
C. Human Intelligence Techniques	20
1. Official Presence	21
2. Other Aspects of the Hostile Intelligence Presence	23
3. Recruited Agents	25
4. Soviet Methods of Recruitment	26
5. Technology Transfer	28
6. Active Measures and Disinformation	30
D. Technical Collection Operations	33
1. Interception of Communications	33
2. Other Forms of Electronic Surveillance	34
3. Penetration of Computer Systems	35
4. Imagery	36
E. Summary	37
III. Counterintelligence	38
A. Need for a Counterintelligence Strategy	39
B. Hostile Presence Limits	40
C. Counterinteiligence Awareness Programs	45
D. Domestic Operations	48
1. Coverage of Establishments and Officers	49
2. Offensive Operations	50
3. Espionage Investigations and Prosecutions	52
E. Overseas Operations	56
F. Personnel Management and Training	56
IV. Security Countermeasures	58
A. A National Strategic Security Program	59
B. Personnel Security	65
C. Information Security	74
D. Communications, Computer and Emanations Security	80
E. Technical and Physical Security	85
F. Industrial Security	87
G. Congressional Security	90
V. Appendixes	97
Appendix A. *U.S.* v. *Whitworth*, Affidavit of RADM William O. Studeman and Declaration of John L. Martin	97
Appendix B. Defense Security Institute Analysis of the Harper Case	105
Appendix C. Defense Security Institute Analysis of the Bell/Zacharski Case	112

Page

Appendix D. Defense Security Institute Analysis of the Cavanagh Case 126

Appendix E. *U.S.* v. *Zakharov*, Affidavit for an Arrest Warrant and Search Warrant; and Indictment 136

Appendix F. Forged letter from Herbert Romerstein to Senator David Durenberger; actual letter from Romerstein to LTG Robert L. Schweitzer; and forged letter from LTG Schweitzer to President Augusto Pinochet of Chile 142

Appendix G. Draft Senate Security Manual 146

99TH CONGRESS
2d Session

SENATE

REPORT
99–522

MEETING THE ESPIONAGE CHALLENGE: A REVIEW OF UNITED STATES COUNTERINTELLIGENCE AND SECURITY PROGRAMS

OCTOBER 3 (legislative day, SEPTEMBER 23), 1986.—Ordered to be printed

Mr. DURENBERGER, from the Select Committee on Intelligence, submitted the following

REPORT

I. INTRODUCTION AND SUMMARY

As espionage is ancient, so is counterintelligence. The Chinese military theorist Sun Tzu stated the principle in the fourth century B.C.: "It is essential to seek out enemy agents who have come to conduct espionage against you. . . ." [1] Today, over two millenia later, the battle is still being waged.

A. BACKGROUND

At the beginning of the 99th Congress, the Select Committee on Intelligence initiated a comprehensive review of the capabilities of U.S. counterintelligence and security programs for dealing with the threat to the United States from Soviet espionage and other hostile intelligence activities. This decision was an outgrowth of eight years of Committee interest in these issues. The review is also consonant with the Committee's mission to "oversee and make continuing studies of the intelligence activities and programs of the United States Government, and to submit to the Senate appropriate proposals for legislation and report to the Senate concerning such intelligence activities and programs." Senate Resolution 400, which established the Committee ten years ago, specifies that intelligence activities include "activities taken to counter similar activities directed against the United States."

The Committee's review had barely begun when the arrests of John Walker and two of his relatives began to make 1985 the "Year of the Spy." In June, 1985, the Committee pledged that it

[1] Sun Tzu, *The Art of War*, trans. by Samuel B. Griffith, Oxford University Press (London: 1963), p. 148.

would prepare a report to the full Senate at the earliest possible time. In light of this Committee's ongoing efforts, the Senate decided not to create a National Commission on Espionage and Security. On June 20, 1985, the Chairman of the Committee wrote to the President, saying, "You and we share an historic opportunity—both to dramatically improve U.S. counterintelligence and security and to demonstrate how Congress and the Executive can work together to achieve progress in sensitive intelligence areas."

The ensuing fifteen months have generated an amazingly sustained interest in counterintelligence and security on the part of both policymakers and the public. There have been over a dozen arrests for espionage, nearly all leading to guilty pleas or verdicts; Americans and West Germans with sensitive information have defected to the Soviet Union and East Germany; and Soviets with sensitive information have defected to the West, and in one major case then returned to the Soviet Union. Most recently, the Soviet arrest of an innocent American journalist in retaliation for the U.S. arrest of a Soviet U.N. employee has made it clear that counterintelligence, while seemingly a peripheral element in superpower relations, can even become the focus of U.S.-Soviet confrontation.

The "Year of the Spy" was characterized by intensive Executive branch attention to problems of counterintelligence and security. Of particular note were the efforts of the Department of Defense Security Review Commission, chaired by General Richard G. Stilwell, USA (retired), and the Secretary of State's Advisory Panel on Overseas Security, chaired by Admiral Bobby R. Inman, USN (retired) and Executive branch steps to implement their recommendations. The Stilwell Commission led to significant progress in Defense Department personnel and information security policies, and the Inman Panel led to restructuring of State Department security functions and a major embassy rebuilding program around the world.

The Committee's efforts have encouraged, and have greatly benefitted from, this sustained Executive branch attention to counterintelligence and security matters. The Committee received an unprecedented level of cooperation from the President, the National Security Council staff, the Intelligence Community Staff, and the many departments and agencies with counterintelligence or security functions. Executive branch experts and policymakers testified in sixteen closed hearings on specific counterintelligence cases and the current state of U.S. programs to counter hostile intelligence activities. Scores of staff briefings and the provision to the Committee of many sensitive Executive branch studies enabled the Committee to compile the very best ideas and recommendations of those in government, as well as suggestions from security experts in industry. The Committee, in turn, evaluated those ideas and submitted a comprehensive set of recommendations for Executive branch consideration.

The Intelligence Authorization Act for FY 1986 included a statutory requirement that the President submit to the House and Senate Intelligence Committees a report on the capabilities, programs and policies of the United States to protect against, detect, monitor, counter and limit intelligence activities by foreign powers,

within and outside the United States, directed at the United States Government. The report was to included plans for improvements that the Executive branch has authority to effectuate on its own, and recommendations for improvements that would require legislation. To assist the Senate Intelligence Committee in its work, the conferees on the Act requested an interim report developed in consultation with the Intelligence Committees. This Committee, in turn, prepared its own interim report, which it shared with the Executive branch last winter.

The many good ideas and recommendations that the Committee obtained from Executive branch officials and studies had not yet been implemented for two basic reasons: counterintelligence and security had failed to receive sustained attention; and the ideas frequently challenged established ways of doing things, cut across bureaucratic lines of responsibility, or required substantial changes in resource allocation. External events provided substantial impetus for interagency attention to these issues. The Committee's efforts and the Executive branch's cooperation are producing the interagency decision-making that is required for progress.

The President began, responding to a request from the Committee, by designating the Director of Central Intelligence to represent the Administration at a series of Committee hearings on counterintelligence and security programs and selecting a counterintelligence expert on the NSC staff as liaison to the Committee. An interagency mechanism under the Senior Interdepartmental Group for Intelligence (SIG–I) supplied coordinated Executive branch reactions to the Committee's interim report recommendations. This not only helped the Committee, but also gave the Executive branch itself the opportunity to address and decide these important policy issues. The resulting positions were conveyed to the Committee in the President's interm report and referred to an NSC staff committee for implementation.

The President's interim report and subsequent consultation between Executive branch officials and the Committee were thus of great value in the preparation of the present Report. The Committee looks forward to receipt of the President's final report, which will serve as an important benchmark of the progress achieved thus far to strengthen counterintelligence and security capabilities.

The summary that follows is based upon the Committee's unclassified public Report. The Committee's full Report to the Senate contains substantial additional material, including findings and recommendations that remain classified.

B ORGANIZATION OF THE U.S. GOVERNMENT TO MEET THE HOSTILE INTELLIGENCE CHALLENGE

The Committee's findings underscore a fundamental challenge to the nation. The hostile intelligence threat is more serious than anyone in the Government has yet acknowledged publicly. The combination of human espionage and sophisticated technical collection has done immense damage to the national security. To respond to the threat, the United States must maintain effective counterintelligence efforts to detect and neutralize hostile intelligence oper-

ations directly, and defensive security countermeasures to protect sensitive information and activities.

The Committee believes that, as a result of significant improvements in recent years, the nation's counterintelligence structure is fundamentally sound, although particular elements need to be strengthened. The Executive branch and the Committee agree on the importance of developing and implementing a coherent national counterintelligence strategy that integrates the work of the FBI, the CIA and the Departments of State, Defense and Justice. Executive branch agencies are already drafting such a document. The Committee expects this strategy to play a major role in its oversight of Executive branch counterintelligence efforts in the years to come.

By contrast, defensive security programs lack the resources and national policy direction needed to cope with expanding hostile intelligence operations. Personnel security policies remain fragmented despite persistent attempts to develop national standards. Information security reforms are long overdue. America faces vulnerability to hostile intelligence activities in the areas of communications and computer security, where countermeasures must keep pace with increasing technological change. Consequently, in December, 1985, the Committee called for the development of a National Strategic Security Program that would address these issues. The Committee believes that a new and more permanent national policy mechanism is needed to create this program and then to coordinate and foster the protection of information and activities having the greatest strategic importance.

In recent months, the Executive branch has come to understand the sense of urgency with which the Committee views the need for an integrated strategic security program and an improved security policy structure. An effort to develop such a security program is now likely. The Director of Central Intelligence, in his capacity as chairman of the Senior Interdepartmental Group for Intelligence, recently revamped the security committee structure under the SIG–I and called for greater participation in those committees by policymakers, so that decisions could be reached on interagency issues and policy initiatives.

The Committee believes that these changes are insufficient because they fail to bridge the gaps between the various security disciplines. Most Executive branch officials, although opposing further changes at this time, do not dispute the likely need for them in the future. The Committee will continue to push for more effective policy review and formulation, for it believes that the national security cannot afford much more delay. This is especially true if the current Administration is to leave as a legacy a workable security policy system that will not have to be reinvented by each succeeding administration. The Committee recommends that the eventual new security policy structure be one that transcends current politics and policy and is codified in an Executive Order.

C. COUNTERINTELLIGENCE: LEARNING THE LESSONS OF RECENT CASES

The Committee has examined in detail each of the espionage cases that have come to public attention in recent years, as well as

the Yurchenko defection case and cases that remain classified. Although this Report does not discuss individual cases in detail, many of the recommendations in sections III and IV reflect lessons learned through those cases.

The first lesson of these cases is the need for greater counterintelligence and security awareness. The Committee found insufficient tailoring of security awareness material to the needs of particular audiences—defense contractors, workers at government facilities, U.S. personnel stationed overseas, members of ethnic groups known to be targeted by foreign intelligence services, congressional staff and others. The usefulness of such material is illustrated by the fact that once the U.S. Navy began to improve its security awareness briefings after the Walker case, co-workers of Jonathan Pollard noted his unusual pattern of document requests and alerted authorities.

The second lesson is the need for earlier involvement of the FBI and the Department of Justice in cases of suspected espionage. When offices or agencies have held back from bringing in the FBI, events have often gotten out of control. When the FBI has been alerted in time, their investigative resources and interview skills have often led to confessions. When the Justice Department has been involved at an early stage, cases destined for prosecution have been built on more solid ground, resulting in numerous convictions.

The third lesson is the need for more attention and better access to information on the finances, foreign travel and foreign contacts of persons with sensitive information. The Committee found that the FBI sometimes lacked access to financial and telephone records in its counterintelligence investigations; that insufficient attention was given to signs of trouble regarding former employees with sensitive accesses; and that too few people were alerting office security personnel or the FBI when they were approached by possible foreign intelligence officers.

The Chin, Pollard and Scranage cases have taught the clear lesson that espionage services outside the Soviet bloc also engage in illegal activities targeted at the United States, which must not be tolerated. The Bell and Harper cases, among many, underscored the need for controls on the activities of certain Eastern European representatives and of U.S. companies controlled by the Soviet Union or its allies. And the Zakharov case, like the Enger and Chernyayev case eight years ago, reminds us that the KGB is willing to use the United Nations Secretariat for intelligence cover.

The Edward Lee Howard case led to investigations and corrective action in the CIA, just as the Walker case led to formation of the Stilwell Commission and to additional steps by the U.S. Navy. The FBI and the Justice Department are still absorbing the lessons of the Howard case. The Committee will continue to monitor how well all the agencies implement improvements in response to those lessons.

The defection and re-defection of Vitaly Yurchenko, which highlighted both the counterintelligence value of defectors and apparent shortcomings in their handling and resettlement, also led to internal reviews and useful actions by the CIA to improve its handling of defectors. The Committee believes that more must be done, however, to change the basic objectives with which the U.S. Gov-

ernment approaches defectors. We must accept the obligation to help defectors succeed in, and contribute to, American society. Executive branch efforts to analyze and learn from the Yurchenko case continue, and the Committee expects to see more progress in this area.

The CIA has taken significant steps to improve recruitment and career development programs for counterintelligence personnel. The Scranage and Howard cases suggest that there was, and is, substantial need for improvement in CIA counterintelligence, and the Committee will continue to monitor CIA efforts. The military services and the FBI are also beginning to improve their recruitment and career development programs for counterintelligence, but progress is uneven.

The Committee will continue to press Executive branch agencies to incorporate into their operations improved counterintelligence awareness and procedures. While agencies have moved in the last year to remedy problems that were exposed in recent espionage cases, they have been much slower to accept the painful need to confront the implications of hostile intelligence successes. Attentiveness to possible hostile knowledge of classified U.S. operations must be increased, and analysis of the impact of known losses of classified information must extend to the unhappy possibility that operations or weapons systems will require modification. While there is always a need not to let worst-case analyses paralyze our military and intelligence services, the greater current danger appears to be a wishing away of the consequences of hostile intelligence efforts.

D. SECURITY COUNTERMEASURES: DEFENDING ON MANY FRONTS

The National Strategic Security Program that the Committee recommends will have to address a multitude of issues, cutting across both agency and disciplinary lines. Thus, different agencies have failed for years to agree upon the scope and methods to be used in background investigations for Top Secret and Sensitive Compartmented Information clearances; the result has been wasteful duplication of investigations. Military services, in particular, have been permitted to establish far too many special access programs, all in the name of security but sometimes with lower security standards than the regular programs maintain. Technical experts who run our nation's computer security programs have poured additional funds into specially-designed hardware and software to protect sensitive computer systems, while doing little to combat the major personnel problem of assuring the reliability of computer users with access to so much sensitive data. The various agencies that deal with technical security issues have only recently begun to forge effective cooperation on approaches to those issues. And this country has a long way to go in the development of operations security practices to protect sensitive programs against hostile intelligence collection activities.

This Report groups many security issues by discipline, but the Committee feels strongly that many, and perhaps most, of those issues will remain unresolved until a more effective security policy structure is implemented. There is a need to upgrade security

across the board, with improved recrutiment, improved training of personnel ranging from security clearance adjudicators to polygraphers and technical security personnel, and upgraded job classifications that reflect the increased importance and sophistication of modern security specializations.

In the field of personnel security, the Committee found, as did the Stilwell Commission, that insufficient attention was being paid to the reinvestigation of those who already have security clearances. Both the Defense Department and the intelligence community now understand the importance of reducing the backlog in those reinvestigations, and the Committee has worked to ensure that the needed funds to accomplish this swiftly are provided in legislation. One reason for recommending interagency agreement on a "single scope" background investigation is the hope that funds thus saved could be put to work on the pressing reinvestigation task, as well as on upgrading Secret clearance investigations as recommended by the Stilwell Commission. The Defense Department has reduced the number of cleared personnel by some 900,000 persons—over 20%—thus also easing some of the clearance investigation costs.

There is a crisis of standards in sensitive governmental positions. The Committee found no rigorous standards regarding the hiring of persons who have committed felonies. Follow-up measures after persons with admitted problems like past drug use are granted clearances are poor or nonexistent. Even the most sensitive clearances are granted to virtually anyone whose record does not contain clear disqualifying factors, rather than being based upon a selection process that chooses those persons most able to cope with the pressures of sensitive access and security. In light of this, the Committee has supported Defense Department efforts to develop counterintelligence polygraph programs with the highest quality controls, pursuant to the test program approved by the House and Senate Armed Services Committees.

The Committee has found that the classification system is unduly complicated and that it breeds cynicism and confusion in those who create and use classified information. The Committee believes that a streamlined system, in which the Confidential classification is eliminated and all information is either Secret or the equivalent of Sensitive Compartmented Information, would be much more workable despite the major changes and initial costs that this would entail.

The Committee also found that authorized (but uncontrolled) disclosures and unauthorized leaks of classified information are so commonplace as to imperil many sensitive programs and operations. Recent Executive branch efforts to investigate instances of unauthorized disclosure of classified information and to punish those responsible are a welcome development. The Committee calls on the Executive branch to go further, however, and to adopt procedures governing authorized disclosures, so that there will be a record of such disclosures—thus relieving the FBI of the need to investigate cases that are not real leaks—and so that those who originate classified information will have a chance to argue against its release. There must be both firmness and order in the information security system before it will gain the respect of the millions of people who handle classified information.

The Committee was pleased to learn of the National Security Agency's many efforts to improve the communications security of the U.S. Government. It supports NSA's plan for the development and licensing for distribution of low-cost secure voice telephone equipment. In addition, the Committee has proposed Fiscal Year 1987 funding to improve communications security by beginning the encryption of many domestic commercial communications satellite links.

The Committee endorses the role of NSA in developing computer security hardware, systems and standards for both the government and segments of the private sector, in cooperation with the National Bureau of Standards. The Committee recommends, however, increased attention to personnel security aspects of protecting computerized information. It supports State Department efforts to place U.S. citizens in charge of the computers in U.S. embassies overseas. The Committee believes that personnel with access to the most sensitive computer systems should be included in personnel reliability programs similar to those now being instituted for persons with sensitive cryptographic access. And it believes that there must be better analysis of information system vulnerabilities before permission is given to put sensitive information in those systems.

The Committee was very concerned over serious deficiencies in the security of U.S. facilities overseas, primarily those managed by the Department of State. The bugging of typewriters in the U.S. Embassy in Moscow graphically demonstrated both Soviet sophistication and U.S. vulnerabilities. Steps are being taken to combat technical penetration efforts, ranging from the embassy rebuilding program proposed by the Inman Panel to an equipment protection program that was funded in the Diplomatic Security Act. The Committee supports these and other efforts, and it has worked to ensure that agencies will work closely with each other to bring the best expertise to bear on technical security problems.

The Committee has also found the industrial security system for classified defense and intelligence contracts to be seriously deficient, to an extent that warrants consideration of major changes. The Committee recommends a pilot program to assign Defense investigative Service personnel to large sensitive contractor facilities on a full-time basis. It proposes changing the Federal Acquisition Regulations to make security a direct cost in contracts, rather than an overhead cost that is inevitably subjected to corner-cutting. It suggests greater incentives in contracts for security performance, as well as a requirement that security officers be trained and government-certified. Many of the Committee's recommendations regarding personnel and information security will also have a direct impact upon industrial security practices.

Attention to security requirements is also needed in Congress itself. The Committee found that there was no centralized registry of Senate personnel with clearances, little or no security awareness material for Congress, and little understanding of how to protect sensitive information that is provided to Member offices and committees. At the request of the Majority Leader, the Committee joined with the Committee on Rules and Administration and the Committee on Governmental Affairs in recommending that a

Senate security office be established to develop and oversee implementation of standards and procedures in these areas. The Committees recommended that the security office be instructed to survey the extent of clearances among Senate staff, to recommend how the number of cleared personnel might be reduced, and to develop a Senate security manual, the provisions of which would be binding on all Members, Officers and employees of the Senate. The Committee continues to work closely with Senate leadership on these efforts, with a goal of creating a security office early in the next session.

E. BUDGETARY IMPACT

The Committee's recommendations will not be cost-free. Some savings would be achieved through streamlining the classification system, adopting common standards for background investigations, and implementing current national policies that lessen the requirement for TEMPEST protection of U.S.-based information-processing equipment. But the Committee believes that the U.S. Government has suffered for years from inadequate investment in security countermeasures.

In the Intelligence Authorization Act for Fiscal Year 1987, the Committee has proposed substantial increases in spending for security in the intelligence community and in related Defense Department programs. Among these initiatives are an additional $129 million for communications security, including the first year of a five-year plan to encrypt sensitive domestic communications satellite channels, and an additional $22 million to improve personnel security in the Defense Department. In 1985, Committee members proposed what became a $35 million supplemental appropriation for improved technical security at U.S. facilities abroad. In 1986, the Congress passed the Diplomatic Security Act and a supplemental appropriation providing funds for a massive program to upgrade security at U.S. missions. This commitment is designed for protection against not only terrorism, but also hostile intelligence penetration.

The additional expenditures recommended by the Committee for FY 1987 would amount to an increase in annual spending for counterintelligence and security of at least $500 million above the funding level in FY 1985. This commitment must continue in the years ahead, when further increases may well be required because of the growing technical, communications and computer security vulnerabilities. From a larger perspective, however, the costs of improved security will be offset by the gains to the United States in the overall U.S.-Soviet balance of military, intelligence, economic and political capabilities. Soviet espionage successes have cost our country or saved our adversaries billions of dollars. Just as our nation's investment in intelligence-gathering programs has a significant payoff for national security, an increased investment in counterintelligence and security programs will help deny comparable advantages to the Soviets.

F. LEGISLATIVE PROPOSALS

The great majority of the Committee's findings and recommendations relate to administrative actions. Some needed actions do require, however, legislative authorization. In these cases, the Committee has either recommended or, often, already introduced the needed legislation.

Members of the Committee have sponsored several pieces of legislation in recent years to bring the hostile intelligence presence in the United States under some control. The Committee recommends that these be implemented so as to maintain a limit of 320 on permanently accredited Soviet embassy and consular personnel. The Committee also found gaps in current legislation and recommended three further steps: a legislated policy of equivalence between the U.S. and Soviet U.N. missions (introduced by Senators Leahy and Cohen as S. 1773); registration of commercial entities controlled by Warsaw Pact governments (introduced by Senator Roth as S. 1900); and extension of the Foreign Missions Act to include commercial and other entities controlled by foreign governments (introduced by Senators Durenberger and Leahy as S. 1947). All three proposals have been attached to the Intelligence Authorization Act for Fiscal Year 1987.

The FBI could benefit greatly from legislation in several areas. The Committee has added provisions to the Intelligence Authorization Act for Fiscal Year 1987 that would require banks and telecommunications companies to comply with FBI requests for access to customer records pursuant to duly authorized full counterintelligence investigations. State privacy laws and fears of civil suits have inhibited some companies from cooperating with the FBI in recent years. The Committee is also prepared to introduce legislation to create a court order system, comparable to that which now exists under the Foreign Intelligence Surveillance Act, to authorize physical searches for couterintelligence purposes. This would avert the need to rely on assertion of inherent Presidential powers in this area and would make it easier to use material thus obtained in eventual prosecutions.

The FBI has a problem in providing sufficient financial incentives to its Agents who must work in New York City, which in turn makes it difficult to retain counterintelligence specialists in that Field Office for substantial periods of time. If the FBI determines that legislation is required to address this problem, the Committee is prepared to work with the FBI to develop a suitable legislative approach.

The Committee recommends that the FBI and the Justice Department develop improved means of prosecuting foreign intelligence officers or agents who enter the United States illegally or under non-official cover and who engage in intelligence support functions without actually passing classified information. This could result in legislative proposals in the next Congress.

Although the Committee has not recommended legislation regarding assistance to defectors, it is quite possible that the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs will make such recommendations when it completes

its inquiry into that matter. The Intelligence Committee expects to work closely with the Permanent Subcommittee on this issue.

The Committee supports recent Defense Department efforts to develop a counterintelligence polygraph program with strict quality controls, modeled on the Air Force's successful Seven Screens program. The Committee recommends that the Armed Services Committee either propose legislation to establish a permanent authority for this polygraph effort or extend the current test program under which DoD is operating and set a date by which the issue of permanent authority will be decided.

Deficiencies in congressional security have prompted the Committee, in conjunction with the Committees on Governmental Affairs and Rules and Administration, to propose that the Senate establish a Senate security office with responsibilities in the areas of personnel and information security. The office would be established by Senate Resolution.

The Committee has not recommended any legislation at this time to deal with the unauthorized disclosure of classified information. It believes that consideration of this issue should be postponed until appeals are completed in the *Morison* case and the applicability of the federal espionage statutes to leaks and other disclosures has been decided. In addition, the Committee believes that there are significant administrative steps that can and ought to be implemented more quickly, in particular the adoption of procedures to govern the authorized disclosure of classified information.

G. RESPECT FOR INDIVIDUAL RIGHTS

A free society cannot allow the fear of foreign adversaries to undermine the constitutionally protected rights that define the true character of our nation. This principle has guided the Committee in its review of counterintelligence and security programs. As President Reagan stated on June 29, 1985:

> [W]e can counter this hostile threat and still remain true to our values. We don't need to fight repression by becoming repressive ourselves. . . . But we need to put our cleverness and determination to work and we need to deal severely with those who betray our country. We should begin by realizing that spying is a fact of life and that all of us need to be better informed about the unchanging realities of the Soviet system. . . . There is no quick fix to this problem. Without hysteria or finger pointing, let us move calmly and deliberately together to protect freedom.

The Committee's recommendations seek to strengthen U.S. counterintelligence and security measures without violating constitutional rights or upsetting the delicate balance between security and freedom. A broad range of improvements can be made without adversely affecting the rights of individuals, and the additional tools needed for counterintelligence and security purposes can be made subject to reasonable safeguards that minimize intrusion into the privacy of American citizens.

II. The Hostile Intelligence Threat

The hostile intelligence threat to the United States is severe, and it confronts the Government and the American people with increasingly serious challenges. The threat spans all types of intelligence operations from traditional human espionage to the most sophisticated electronic devices. Every kind of sensitive information is vulnerable, including classified government information, emerging technological breakthroughs and private financial transactions. Foreign intelligence services also sometimes target the political process, seeking both information and influence.

What has made the threat more vivid to the Congress and the public are the many espionage cases that surfaced publicly in the last few years. During 1984–86, twenty-five people have been convicted or have pleaded guilty to charges of spying against the United States. Another person charged with espionage, Edward Lee Howard, has defected to the Soviet Union; a Soviet employee of the United Nations has pleaded "no contest" to espionage charges; and several foreign diplomats have been detained and/or ousted because of their espionage activities. The upsurge in espionage prosecutions began in the late seventies; and FBI Director William H. Webster said in 1984 that the espionage cases that came to public attention were "merely the tip of the iceberg." The Committee believes it is vital for the Senate and the public to be aware of the full dimensions of the threat, technical as well as human.

A. Damage to National Security

National policymakers must recognize as clearly as possible the extent and gravity of the damage to national security interests caused by hostile intelligence operations. Based on the public and classified record, the Committee has found the aggregate damage in recent years to be far greater than anyone in the U.S. Government has yet acknowledged publicly. The Committee has reviewed the actual and probable injury resulting from recent espionage cases, technical security compromises and technology transfer. The inescapable conclusion is that the damage was immense:

U.S. military plans and capabilities have been seriously compromised;

U.S. intelligence operations were gravely impaired;

U.S. technological advantages have been overcome in some areas;

U.S. diplomatic secrets were exposed to the scrutiny of our adversaries; and

Sensitive aspects of U.S. economic life were subject to constant Soviet monitoring.

Foreign intelligence services have exploited human and technical vulnerabilities to penetrate some of the most vital parts of our defense, intelligence and foreign policy structure, including many Executive branch agencies and the Congress. A sober examination of the damage is essential to make rational decisions on policy initiatives and resources allocation for counterintelligence and security programs.

In assessing the military damage, the Committee agrees with an estimate by a senior FBI official that the espionage cases over the

past several years have involved billions of dollars of actual and potential damage to U.S. military programs. The cases primarily include John Walker and Jerry Whitworth, James Harper, William Holden Bell, Thomas Cavanagh, Christopher Cooke and Ernest Forbrich.

Walker-Whitworth

Although the assessment in the Walker and Whitworth cases is still incomplete, their information may have enabled the Soviets to read some of the U.S. Navy's most secret messages to the fleet from the 1960's to the time of their arrests in 1985 and also possibly reduced the U.S. lead in anti-submarine warfare. The cryptographic material passed by John Walker and Jerry Whitworth was exceptionally harmful, because the Soviets could use it to decipher encrypted U.S. Naval communications. Vitaly Yurchenko, the Soviet KGB defector who later returned to the Soviet Union, told U.S. authorities that the Soviets read over a million coded messages as a result.

(An official assessment of the damage, prepared by the Director of Naval Intelligence and a senior Justice Department official, is provided in Appendix A.)

Harper

In 1979–81 James Harper passed to Polish intelligence a huge array of materials pertaining to the survivability of the Minuteman missile system and to U.S. defenses against ballastic missile attack. He obtained the information from a private firm doing contract research for the U.S. Army Ballistic Missile Defense Advanced Technology Center in Huntsville, Alabama. Harper received approximately $250,000 for documents whose loss Army experts have rated as "beyond calculation." He also provided computer data-base tape available through his contacts in Silicon Valley. Harper's largest single delivery occurred in 1980, when he took some 100 pounds of classified reports to Warsaw, where a team of 20 KGB experts flown in from Moscow declared them to be extremely valuable. KGB Chairman Yuri Andropov commended the Polish intelligence unit handling Harper for its efforts. (An account of the Harper case prepared by the Defense Security Institute is provided in Appendix B.)

Bell

William Holden Bell was recruited by a Polish intelligence officer operating under commercial cover. As a project manager in the Advanced Systems Division, Radar Systems Group at Hughes International Corporation, Bell was responsible for development and promotion of the radar fire control product line of tank vehicles. From 1978 to 1981, Bell supplied Polish (and presumably Soviet) intelligence extensive classified documents on the Covert All-Weather Gun System [CAWGS], a proposed tank gun using Low Probability of Intercept Radar [LPIR] or "quite radar." LPIR uses a disguised radar signal that is difficult for enemy targets to identify as radar; an enemy is thus prevented from taking evasive action or using the radar signal for directing return fire. (An account of the

Bell-Zacharski case prepared by the Defense Security Institute is provided in Appendix C.)

Cavanagh

The defense contractor case with the greatest potential for devastating harm involved Thomas Cavanagh, an engineer at Northrop Corporation. He was arrested in December, 1984, for attempting to sell classified documents on Stealth technology to the Soviets. The FBI intercepted his attempt, and FBI agents posing as KGB officers made the arrest after giving him $25,000 for the documents. While no serious compromise actually occurred, FBI Director Webster has said that Cavanagh's documents contained "the core of the Stealth technology" which had "cost this country over $1 million an hour to develop." (An account of the Cavanagh case prepared by the Defense Security Institute is provided in Appendix D.)

Cooke

Lt. Christoper Cooke, deputy commander of an Air Force Titan missile crew, was charged with passing classified information to the Soviets on U.S. strategic missile capabilities in 1980–81. While the damage was serious, the charge was dismissed because Air Force prosecutors had offered him immunity to find out if he was a part of a larger spy ring (which he apparently was not).

Forbrich

Ernest Forbrich, a West German auto mechanic, was arrested in 1984 in Florida after buying a classified military document from an undercover agent posing as an Army officer. Forbrich appears to have been a conduit who passed U.S. military secrets to East German intelligence, and he admitted selling documents to the East Germans for 17 years. Forbrich traveled frequently to the United States, contacting former U.S. military personnel who had served in West Germany. Although he was convicted of espionage, none of the former U.S. military personnel whom Forbrich contacted was charged.

The espionage damage to U.S. intelligence over the past decade has been as great as the harm to military programs. The cases that surfaced in 1985—Howard, Pelton, Chin and Pollard—represent a severe blow to U.S. intelligence, with Howard, and Pelton doing the greatest harm because they compromised collection efforts directed at high-priority targets in the Soviet Union. Other recent cases involved FBI Agent Richard Miller, Army counterintelligence specialist Richard Craig Smith, and CIA employees Sharon Scranage and Karl Koecher.

Howard

Edward Lee Howard, a former case officer dismissed by the CIA, was accused of selling intelligence secrets to the Soviets and subsequently defected to Moscow. Howard probably gave the Soviets information on sensitive CIA operations in Moscow.

Pelton

Ronald Pelton, a former communications specialist with the National Security Agency from 1965 to 1979, was convicted in 1986 of selling the Soviets information about a highly classified U.S. intelligence collection project targeted at the Soviet Union. Other aspects of the damage caused by Pelton that did not surface at the trial have not yet been completely evaluated.

Chin

Larry Wu-tai Chin gave the Chinese an inside view of U.S. intelligence reporting on China and related topics for decades, first as a translator for the U.S. Army and then as a translator and foreign media analyst for the CIA. Chin was a "plant" who received intelligence training before his employment by the Army in 1943. His reporting was highly praised by Chinese officials.

Pollard

Jonathan Jay Pollard, a civilian intelligence analyst with the Naval Investigative Service, pleaded guilty in 1986 to the charge of illegally passing classified documents to Israel. Pollard obtained a wide array of intelligence reports on the Middle East for his Israeli contacts.

Miller

FBI Agent Richard Miller injured the entire intelligence community, not just the FBI, when he provided the Soviets in 1984 (through his Russian emigre lover Svetlana Ogorodnikova) a document outlining overall U.S. foreign intelligence collection priorities.

Smith

Richard Craig Smith, a former Army counterintelligence agent, was charged in 1984 with selling information to Soviet agents in Tokyo identifying U.S. double agents being operated against Soviet intelligence. Smith was acquitted in 1986 after asserting as his defense that be had been working under the direction of CIA operatives in Honolulu.

Koecher

Karl Koecher, a naturalized U.S. citizen of Czech origin, worked as a translator for the CIA in the 1970s. He and his wife were arrested in 1984 as they prepared to fly to Switzerland. By then, the FBI had sufficient information to establish that Koecher was trained and sent to the United States in the 1960s to work as a Czech "illegal" and penetrate U.S. intelligence. Koecher was able to give Czech intelligence everything he knew about such sensitive CIA information as he was provided in his job as a translator.

Scranage

Sharon Scranage, a CIA operations support assistant in Ghana, was convicted in 1985 of turning over classified information, including the identities of CIA case officers and clandestine sources, to Ghanaian intelligence officials.

In addition to the damage to classified U.S. military and intelligence programs, hostile intelligence services have acquired sensitive technological data in the United States, Western Europe, Japan and elsewhere. Soviet acquisition of U.S. technology has significantly reduced the time it took the Soviets to develop new weapons systems and field countermeasures to U.S. systems. A recent example is the case of Manfred Rotsch, a Director of Planning for a prominent West German aerospace company, who was arrested as a Soviet agent. Rotsch was in a position to transfer detailed manufacturing information on Western weapon systems to the KGB, and the case points up the vulnerability of U.S. advanced technology released in coproduction or licensing programs. The research and development cost savings to the Soviet Union from illegal Western technology acquisition are believed to be enormous. The Ministries of Defense Industry and Aviation Industry alone are estimated to have saved half a billion rubles (roughly $700 million at official conversion rates) between 1976 and 1980, although that figure probably reflects operating cost savings as well as R&D.

In the diplomatic field the recent discovery of bugged typewriters in the U.S. embassy in Moscow exposed an operation of some duration. For years, the Soviets were reading some of our most sensitive diplomatic correspondence, economic and political analyses, and other communications.

More difficult to assess, yet with enormous danger to the United States, is the Soviet interception of U.S. communications from collection facilities throughout the world, including Soviet diplomatic establishments in the United States and an extensive site at Lourdes, Cuba. The Soviets could monitor many U.S. domestic telecommunications channels, including most satellite links and certain ground-to-ground transmissions. While the risk to military secrets from poor communications security is widely understood, the U.S. business community is also highly vulnerable.

Taken together, the damage to national security from espionage, technology theft and electronic surveillance amounts to a staggering loss of sensitive information to hostile intelligence services. As an open society, the United States already allows its adversaries unfettered access to vast amounts of information that must be shared widely so that our political system can function democratically and the process of free scientific inquiry can be most productive. Our openness gives hostile intelligence services the ability to focus their efforts on those few areas of our government and society where confidentiality is required.

The following discussion of the hostile intelligence threat to the United States is designed to give the Senate and the American people a better appreciation of the challenges we will continue to face in the future. It is based upon an assessment prepared by the intelligence community at the Committee's request. By understanding the nature and scope of ongoing hostile intelligence efforts, public officials and private citizens alike can better understand why the Committee recommends increased emphasis on counterintelligence and security programs. There is much that the ordinary citizen can do to strengthen the nation's defenses, especially if the individual works for the federal government, a government con-

tractor, or a high-tech industry or research program. The key requirement is knowledge of the dangers.

B. SOURCES OF THE THREAT

Among foreign intelligence services, those of the Soviet Union represent by far the most significant intelligence threat in terms of size, ability and intent to act against U.S. interests. In fact, the activities of the Warsaw Pact country and Cuban intelligence services are primarily significant to the degree that they support the objectives of the Soviets. The threat from intelligence activities by the People's Republic of China (PRC) is significant but of a different character, as explained below. The intelligence activities of North Korea, Vietnam and Nicaragua pose a lesser, but still significant, threat to U.S. foreign policy interests, although these countries have only a limited official presence in the United States.

Many other countries—hostile, allied, friendly and neutral—engage in intelligence operations against the United States. While these activities cannot be ignored, they do not represent a comparable threat. Nonetheless, in 1985, arrests for espionage included U.S. Government employees who had passed classified information to Israel and to Ghana.

1. Soviet Union

The KGB and the GRU are the two principal Soviet intelligence organizations. The KGB (or Committee for State Security) maintains internal security in the USSR and, as a secret intelligence service, collects intelligence and conducts covert political influence operations (termed "active measures") abroad. The GRU (or Chief Directorate for Intelligence) is the Soviet military intelligence organization and engages only in foreign intelligence activities.

In no other country in the modern world have intelligence and security services played such a crucial, long-term role in sustaining a government and controlling its citizens. In recent years, the KGB has become a vital tool for protecting the Communist Party at home and implementing its policies worldwide, especially through energetic espionage and covert action operations both against Western governments and in the Third World. (Covert action efforts are coordinated with the International Department of the Communist Party, which has lead responsibility for worldwide Soviet "active measures," including propaganda and political influence operations.) Soviet military intelligence came into its own during and just before World War II, and the GRU aggressively supplements the KGB with espionage and massive technical surveillance operations. The GRU coordinates and supports Soviet SIGINT and overhead photography and trains foreign revolutionary cadres and insurgents. In the operational Soviet military, "Spetsnaz" (Special Forces) units have an overseas role as special-purpose commando forces capable of covert infiltration, sabotage and assassination operations.

The highest Soviet collection priority is accorded to policy and actions associated with U.S. strategic nuclear forces. Other high priority subjects are key foreign policy matters, congressional intentions, defense information, advanced dual-use technology, and

U.S. intelligence sources and methods. The Soviets also target NATO intensively, partly as a means to obtain U.S. foreign policy and military information; recent arrests in West Germany and Greece are indicative of the successes of the USSR in targeting U.S. and NATO classified weapons systems.[2] The Soviets heavily influence the collection activity of the Cuban and Warsaw Pact services, in effect expanding their own collection resources through exploitation of the ethnic ties that other services can use in their recruitment efforts, as well as the normally less stringent U.S. controls on the activity of non-Soviet visitors and representatives.

The Soviets acquire much of the information they need through non-clandestine means—diplomatic activities, trade representatives, visitors, students, and other open inquiry. They carefully select participants in exchange programs to maximize access to information of intelligence interest. The Soviet government also has access to computerized U.S. and other Western reference systems, to U.S. Government programs designed to facilitate legitimate dissemination of information, and to open literature ranging from technical journals and industry publications to the news media. Soviet collection efforts are further aided by the absence of effective U.S. Government controls over foreign visitors and indirect exports.

The Soviets aggressively screen information on Western technology to avoid technological surprise and to improve their economy and weapons systems. The methods used to acquire technology will depend largely on the cost and the risk involved. It is likely that increased controls on trade with the Soviets and on Soviet visitors and official personnel will cause changes in Soviet collection techniques. Thus, more use of clandestine methods to acquire technology is likely when it cannot be obtained in other ways.

2. Warsaw Pact and Cuba

The intelligence services of Poland, East Germany, Czechoslovakia, Bulgaria, Hungary and Cuba not only serve their own national interests, but also act as surrogates for Soviet intelligence. While a member of the Warsaw Pact, Romania has looser ties to the Soviets in the intelligence arena. Recent cases demonstrate the aggressiveness of the Warsaw Pact services. In 1983, an employee of the Bulgarian trade office in New York was arrested for espionage based on evidence that he bought a secret document on security procedures for American nuclear weapons. The Bell and Harper cases illustrated the effectiveness of Polish intelligence in penetrating U.S. defense industry. East German agents arrested in the United States over the past three years include a women courier in a KGB espionage network and a prominent scientist attempting to recruit American scientists.

The recent interagency report on Soviet Acquisition of Militarily Significant Western Technology documents fully the relationship between Soviet intelligence and the Warsaw Pact services. The

---

[2] This Report concentrates upon the direct hostile intelligence threat to the United States and does not include the counterintelligence and security implications for the United States of hostile intelligence activities that target U.S. allies or alliances. The Committee will examine these matters in its continuing oversight of U.S. counterintelligence and security programs.

KGB, more than the GRU, relies on the collection capabilities of the East German, Polish, Bulgarian and Czech services. The success of the East European services can be attributed partly to the Western misperception that their countries are less of a threat than the USSR. East European nationals operating in most Western countries have fewer (or no) travel restrictions and, in some cases, find it easier to work in a Western cultural and commercial environment. At the same time, however, the West also has easier access to Warsaw Pact countries than to the Soviet Union. Reciprocity considerations limit the West's ability to impose extreme controls on East Europeans.

The Cuban DGI has long been under the direct influence of Soviet intelligence. While in recent years the Cubans have emphasized operations against anti-Castro emigre groups and illegal acquisition of embargoed U.S. technology and equipment, Cuban intelligence also targets U.S. Government plans and intentions, especially regarding Latin America. There are indications, dating back many years, of Cuban support and training for Puerto Rican terrorists and of propaganda operations to influence segments of American public opinion.

3. People's Republic of China

The PRC has several intelligence services whose personnel are represented among the approximately 1,500 Chinese diplomats and commercial representatives located at some 70 PRC establishments and offices in the United States. They also have some access to the approximately 15,000 Chinese students and 10,000 individuals arriving in 2,700 delegations each year. PRC intelligence also seeks to exploit the large ethnic Chinese community.

The implications of PRC intelligence activities are markedly different from those of the Soviet Union and its surrogates. The forces of the Warsaw Pact are arrayed against those of NATO; and the Soviet Union's expansionist policy poses a current and continuing global challenge to the United States and its allies. The PRC is not now in strategic competition with the United States. Indeed, the United States has fundamental interests in maintaining friendly relations with the PRC and promoting its modernization, to include selective upgrade of its military defensive capabilities. Intelligence collection priorities of the two major communist powers reflect their respective foreign policies. The Soviet intelligence services have urgent requirements with respect to U.S. plans, intentions and capabilities, as well as technology; the PRC services concentrate primarily on advanced technology not approved for release so as to further PRC military and economic modernization in the 1990s and beyond.

Despite these differences, the PRC intelligence threat continues to be significant. The evidence of PRC espionage in the Chin case and from other counterintelligence sources justifies alerting American citizens to the current risks. The recent detention of a British national employed by the New York Times as a reporter in China reflects an increased emphasis by PRC intelligence and security services on surveillence of foreign visitors. PRC efforts to cultivate Chinese-Americans in scientific and technical fields should be recognized as including potential intelligence approaches, as long as

the PRC continues to mount espionage operations against classified U.S. programs and embargoed technology.

4. Other Countries

Other countries also conduct human intelligence operations in the United States, both overt and covert. Their targets include largely the same range of interests as those of the Soviets and the PRC, including high technology and political, military and economic policies and intentions that might affect the particular country.

Among the common activities of foreign intelligence services in this country are attempts to penetrate emigre communities. A large number of expatriate political and emigre groups in the United States are viewed as a threat by authorities in the former homelands. From a national security viewpoint, these activities are less significant than those of the USSR and its allies, although they are clearly in violation of U.S. sovereignty and may have an effect on the U.S. political system. Foreign intelligence services also target ethnic groups in the United States, directly or through front organizations, to influence U.S. decisions on foreign aid, trade agreements and other issues where foreign governments have strong interests.

Two recent incidents illustrate the threat from non-communist governments. In 1984, a vocal opponent of the current regime in Taiwan was murdered in California, and the Taiwanese government later admitted that officials of its intelligence service were implicated. Also in 1984, the South African military attache was expelled from the United States for activities incompatible with his diplomatic status. In 1978, the Committee issued a public report on Activities of "Friendly" Foreign Intelligence Services in the United States which examined, as a case study, South Korean operations in the early-to-mid 1970s. The Pollard case has raised questions as to whether the Israeli government, or significant elements thereof, have engaged in more extensive espionage operations in the United States. While the strategic threat in such cases in less than from Soviet bloc or PRC operations, the harm to specific U.S. foreign policy interests and legal safeguards is still substantial and unacceptable.

C. HUMAN INTELLIGENCE TECHNIQUES

The hostile intelligence threat can be divided roughly between the human side and the wide array of technical collection operations. The human dimension begins with the trained intelligence officer, dispatched under official or nonofficial cover to operate abroad. Intelligence officers recruit and handle agents employed by foreign governments, industries, or political organizations; and they "co-opt" other members of their own government and citizenry for particular assignments. In general, hostile intelligence HUMINT operations fall into the following categories:

"Legal" operations are conducted by intelligence officers under official cover. The term does not mean "lawful," because case officers recruit and handle espionage agents. The FBI estimates that at least 30% of the 1,500 Soviet officials in the U.S. are KGB or GRU staff officers. Reportedly, over 3,000 KGB of-

ficers and approximately 1,500 GRU officers are posted outside the Soviet Union.

"Illegals" are trained intelligence officers sent abroad, often with false identities, who maintain no overt contact with their government. The number of Soviet illegals and their activities are very difficult to estimate.

"Co-optees" are officials or visitors tasked to do particular tasks, such as spotting potential recruits or servicing drops. Many Soviet officials are co-opted, as are many official visitors and some emigres.

"Agents" are American or third-country nationals recruited for current operational purposes or, in some cases, as "sleepers" to be activated at a later date. Apart from the agents surfaced publicly in espionage or illegal export cases, the FBI has numerous other suspected agents under investigation.

Despite the development of increasingly sophisticated technical means of collection, the human agent continues to be the most important key to satisfying a nation's intelligence needs. An intelligence community study summarized the human threat in the following terms:

> The Communist countries depend to a large degree on their human collection networks throughout the world to satisfy their U.S.-related intelligence requirements—requirements ranging from acquisition of advanced technology, location and determination of the quality of strategic and conventional military forces, and assessment of U.S. reaction to international political incidents, to discovery of techniques used by U.S. counterintelligence.

An analysis of hostile human intelligence operations against the United States must address the role of the Soviet-bloc official presence in the United States; the non-official United Nations and "illegal" hostile presence; the recruitment of agents; the Soviet Union's systematic technology acquisition program; and covert political action operations (or "active measures").

1. Official Presence

The spearhead of the Soviet, other Warsaw Pact and Cuban intelligence collection effort is their official presence in the United States. In 1985, there were about 4,250 diplomats, commercial officials and other representatives from Communist countries in the United States, 2,100 of whom were from the Soviet Union and the other Warsaw Pact countries. The Soviet Missions to the United Nations in New York have approximately 275 accredited diplomats; the Department of State has recently mandated a reduction in this number to 170 by April 1988. The Soviets have 320 accredited personnel at their Embassy in Washington and Consulate General in San Francisco, in comparison to the approximately 200 American diplomatic personnel assigned to the Soviet Union. Additional Soviets come to the United States on temporary assignment, as do American personnel to the USSR.

The FBI estimates that at least 30 percent of the Soviet bloc officials and representatives in the United States are professional intelligence officers of the Soviet KGB and GRU or one of the other

East European intelligence services. Under diplomatic cover, Soviet bloc diplomatic personnel accredited to the United States and to the U.N. missions in New York have complete immunity from criminal prosecution for espionage. (By contrast, Soviet nationals employed by the U.N. Secretariat, such as Gennadiy Zakharov, do not have such diplomatic immunity.)

Soviet bloc use of official representatives for espionage purposes is well documented. In the Walker and Miller cases, Soviet officials involved with handling American agents left the country shortly after their agents were arrested. In other instances, successful U.S. counterintelligence operations have led to the exposure of Soviet officials engaged in clandestine communications with agents, such as by servicing "drops." Soviet bloc intelligence officers under diplomatic cover also seek to use overt contacts with Americans as an opportunity to develop long-term relationships providing an opportunity to assess and exploit vulnerabilities for espionage recruitment purposes. In one case in the early 1980s, a Soviet official who attempted to recruit a Congressional staff member was expelled from the country. The staff member had reported the approach and cooperated with the FBI's investigation, which led to exposure of the Soviet official's intelligence recruitment efforts.

The sheer volume of intelligence activity is increased by the number of officials from other Communist countries in the United States as well as the large number of establishments from which they can operate. Soviet bloc and PRC establishments—government offices and U.N. missions—are located in seventeen different cities. The largest numbers are in New York (92), Washington (34), Chicago (11), San Francisco (9), Houston (9), and Newark (9). While most officials are concentrated in New York and Washington, all but the Soviets are allowed to travel almost anywhere they wish in the country, subject to notice requirements and certain other conditions under the Foreign Missions Act in the case of most Warsaw Pact countries.

Within the Soviet services, GRU personnel are targeted primarily against military and scientific and technical information, while KGB personnel in its First Chief Directorate (foreign intelligence) are assigned to one of four operational departments or "lines"—Scientific and Technical (Line X), Political (Line PR), Counterintelligence (Line KR), or Illegals Support (Line N). S&T personnel specifically target U.S. advanced technology. Often, clandestine collection of S&T information is preferred over buying or developing technology because it is cheaper and provides the best short-term results, although there is a risk factor in theft. KGB Line PR officers target governmental policy information and, frequently, seek to advance Soviet objectives via contacts with persons of influence or through covert activities. Certain Line PR officers focus specifically on the Congress. Line KR officers have the security responsibility for preventing defections of Soviet personnel and particular concern for penetration of the U.S. intelligence community, although all lines are tasked with this important function as a matter of general concern. "Illegals" support personnel comprise a small group that helps maintain those networks.

2. Other Aspects of the Hostile Intelligence Presence

The Soviet Union is effectively using U.N. organizations, particularly the Secretariat, in the conduct of its foreign relations and as a cover for the activities of Soviet intelligence officers and co-optees. The United Nations employs, worldwide, approximately 800 Soviet nationals as international civil servants, with about 300 of them in New York. Approximately one-fourth of the Soviets in the Secretariat in New York are considered to be intelligence officers, and many others are co-optees who have been told to respond to KGB and GRU requests for assistance. The Soviet intelligence services also use their developed agents in the United Nations to collect information on U.N. activities; to spot, assess and recruit American and foreign-national agents; to support worldwide intelligence operations; and to collect scientific and technical information on the United States.

The KGB has succeeded in infiltrating its officers into the U.N. bureaucracy, with some reaching positions of authority. The KGB has held the position of Assistant to the Secretary General since Viktor Lesiovskiy held the post under U Thant. The current Assistant is a KGB China expert. The Soviets take full advantage of U.N. personnel procedures such as liberal sick leave. This permits KGB U.N. employees to be absent as often as they desire, enabling them to carry out intelligence activities further abetted by the comparative freedom of movement enjoyed by U.N. employees.

While the State Department has recently required Soviet U.N. employees to give notice of unofficial travel outside the New York area, they are not subject to the geographical off-limits restrictions placed on Soviet diplomats in response to equivalent restrictions placed on travel by U.S. diplomats in the Soviet Union. Little can be done about the number of Soviets employed by the United Nations in view of the large number of Americans similarly employed.[3]

There have also been reports of the U.N. Secretariat being used for clandestine activity by Warsaw Pack officials. Currently, State Department conditions for travel in the United States by U.N. Secretariat employees from the Soviet Union still do not apply to U.N. employees from other Warsaw Pact countries.

The hostile intelligence threat is further expanded by the number of Soviet bloc commercial entities in the United States that can be used as cover for clandestine collection activities. These commercial establishments include the USSR's AMTORG and INTOURIST, the Polish-American Machinery Company (Polamco), and similar East German, Czechoslovak and other East European entities. Through their legitimate business activities, intelligence officers in those firms have access to Americans in business, industry and government who are potential targets for agent recruitment. A Czech, Pole or other East European is frequently able to contact U.S. companies without arousing the suspicion that contact by a Soviet official would occasion. The primary interests of hostile collectors operating under commercial cover are economic data and

[3] For a more detailed discussion of the Soviets at the United Nations, see the Committee's report on *Soviet Presence in the U.N. Secretariat*, S.Rpt. 99-52 (May, 1985).

advanced technology. Altogether, nearly 70 U.S.-chartered corporations, although owned by Warsaw Pack countries, function legally as U.S. corporations and thus are subject to few restrictions on acquiring technologies. East Europeans employed by these firms are subject to no travel controls or notice requirements.

In addition to the threat posed by their official establishments, U.N. employees and front companies, hostile intelligence services have infiltrated intelligence collectors into the United States among the thousands of exchange students, commercial and cultural visitors, tourists and ship crewmen who enter this country each year. Some 2,000 Soviets come to the United States each year under the auspices of the Soviet Academy of Sciences, the Ministry of Trade, the State Committee for Foreign Economic Relations, and other Soviet agencies. They collect not only overt information for non-defense industries, but also classified and proprietary data, in response to intelligence tasking on behalf of military research projects. The number of U.S. universities and institutes subject to focused Soviet efforts reportedly increased from 20 to over 60 from the late 1970s to the early 1980s.

Soviet trade or scientific representatives travel to California about four times a month in delegations ranging from two to ten people, supplementing the 41-person staff of the Soviet San Francisco Consulate. It is reasonable to assume that, just as 30–40 percent of the personnel in each Soviet establishment are intelligence officers, the same percent of the personnel in a Soviet visiting delegation are intelligence officers and/or co-optees. Thus, the Soviets are able to target more intensively the 1,500 high-technology companies in the area known as "Silicon Valley," which constitute the largest collection of electronics and computer manufacturers in the United States.

In recent years, a number of intelligence agents of the USSR, Cuba and other countries have been uncovered among the flood of immigrants into the United States from Communist countries. While not all of these agents are considered classic "illegals," investigations have determined that many have been sent with intelligence missions.

The deep-cover "illegals" dispatched to the United States in the emigre flow and through other means by Soviet bloc and PRC intelligence services represent a particularly perplexing problem because of their completely clandestine manner of operation. They generally enter the United States under false identities with forged or stolen documents. They often acquire U.S. citizenship, and they have attempted to assume the appearance of ordinary Americans having no connection with their home country and intelligence service.

An example of a KGB illegal agent was disclosed publicly by the FBI in 1981. Col. Rudolf Hermann (a pseudonym) had earlier been identified and recruited to work as a U.S.-controlled double agent. Hermann's 25-year career with the KGB had begun in the 1950s while he was serving in the military of a Soviet-bloc country. His initial training in espionage techniques such as secret writing and cipher systems took place in East Germany. More advanced training was received in the Soviet Union.

Before coming to the United States, Col. Hermann practiced his intelligence skills in West Germany and Canada. He and his family entered the United States illegally in 1968, and he established a home and found work as a free-lance photographer. He did not directly collect classified information, but performed support functions such as locating drop sites for other agents and spotting potential recruits. He was also prepared to conduct more active collection operations in the event of the expulsion of Soviet officials in time of crisis or war. Col. Hermann's son had enrolled in an American college, under KGB orders, and was preparing to seek U.S. Government employment, possibly in a sensitive position.

3. Recruited Agents

Visitors and emigres are no substitute for recruited agents inside sensitive U.S. programs. The spy of the 1980s has been described as a new breed, motivated more by greed than by ideology. However, the cases uncovered in 1985 suggest more complex motivations; political beliefs, intrigue, and job dissatisfaction or alienation also appear to have been reasons for engaging in espionage. Most Americans arrested for espionage in recent years actually volunteered their services to the other side.

Soviet intelligence efforts include active programs outside the United States against U.S. Government personnel and businessmen. Even those recruited agents who live in the United States are frequently met in third countries to avoid U.S. domestic counterintelligence. Vienna, Austria, was used as the meeting place for John Walker, Ronald Pelton and Edward Howard.

KGB residencies abroad target principally American embassy employees with access to classified information. Other targets include American journalists, businessmen, and scientists who can furnish sensitive technological information, as well as students with job prospects in sensitive positions for long-range development.

The widespread use of foreign nationals in U.S. embassies and consulates compounds the problems faced by U.S. intelligence in most hostile countries. Over 9,800 foreign nationals are so employed for a number of reasons, including cost considerations. Despite their value in dealing with local government organizations because of their language fluency and understanding of local customs and regulations, their threat to the security of U.S. operations must be recognized.

The employment of foreign nationals in U.S. establishments in the Soviet Union and other Eastern European countries, as well as in numerous other countries where the Soviet bloc has influence, affords hostile security services the opportunity to conduct a variety of observations of U.S. personnel and technical penetrations of U.S. facilities. The foreign nationals' personal observations are used by the KGB to assess possible recruitment targets among the American personnel (e.g., those with financial, family, alcohol, or drug problems), as well as to identify U.S. intelligence personnel. The U.S. Embassy in Moscow faces particular problems in this regard. Soviet nationals operate the carpool, including making mechanical repairs and, until recently, operated the telephones, cleaned the offices, and performed all the maintenance tasks in the

embassy compound. Approximately 200 Soviets are employed at the embassy, contrasted to fewer than a dozen Americans in the Soviet establishments in Washington. The Soviets strictly limit the use of local hires in their own embassies—apparently concerned that if they can succeed, so could U.S. intelligence.

U.S. military installations and personnel abroad continue to attract major Soviet intelligence interest, both to gain potential access to military plans and to acquire sensitive technical data. It is probable that third-country nationals are used to target U.S. bases, just as they are at embassies. There are over 120,000 third-country nationals employed at such installations; and 930 of these have accesses, of which 371 are at the Secret level, to see certain classified material.

4. Soviet Methods of Recruitment

A study by the Defense Security Institute outlines some of the most common Soviet methods of recruiting and handling agents. The agents who steal most of the U.S. classified information lost through human espionage are not foreign nationals, legal or illegal, but Americans already employed in sensitive positions who are recruited, or who volunteer, to provide information to hostile intelligence services.

Social occasions and situations are a favorite hunting ground for Soviet bloc intelligence officers, such as diplomats or U.N. employees, on the look-out for potential recruits. So are restaurants, bars and clubs in the vicinity of defense contractor facilities. The intelligence officer looks for a combination of access to desired information and some motivating factor or factors that might be exploited for drawing a person into espionage. Ideological affinity is not frequently encountered, although it is a desired inducement. Blackmail is a last resort. The most common motivation is financial gain, often combined with conscious or unconscious anger at the employer.

In typical fashion, an intelligence officer proceeds with his cultivation of a prospect by stages, attempting to establish a pattern of payment for seemingly harmless services. The aim is to avoid scaring off the prospect with premature demands for classified information. After classified material is passed, the officer may shift the mode of communication from personal meetings to more secure methods such as "dead drops"—that is, the placement of a package in an inconspicuous agreed location where it can be picked up by the recipient at a later time.

Recruitment of this sort is a process of salesmanship, almost of seduction. Soviet intelligence officers vary in their skill, but some possess the finesse to do an effective job of cultivation without rushing the potential agent. Most of our information concerns the least successful recruitment attempts, such as those reported by persons who become FBI-controlled double agents. KGB training documents, however, describe instances of successful recruitment involving bribery of employees with sensitive access.

In one case cited in KGB training materials, an intelligence officer spotted a possible recruit while serving as interpreter for a Soviet scientist visiting the laboratory of a private U.S. company. The KGB account states that the scientist was aware of his inter-

preter's intelligence function and actively assisted him in that role. The intelligence officer's attention was drawn during the visit to a young lab assistant who seemed poorly dressed. When the Soviet scientist offered to provide copies of a number of his writings to the head of the laboratory, it was revealed that this assistant was studying Russian and could assist in translating the material.

On this basis the Soviet intelligence officer was able to cement an acquaintance with the young worker during the deliberately prolonged process of delivering the documents to the laboratory. As suspected, the lab assistant was having financial difficulties. He was married and attending graduate school and his job was a low-paying one. The KGB officer developed a friendship with him over the course of three months and then began requests for unclassified information in return for payment. Ultimately he persuaded the lab employee to join him in the formation of a consulting firm for the sale of scientific data, which the lab assistant would obtain and the KGB officer would market. In furtherance of this business venture, the lab assistant was persuaded to provide secret as well as unclassified information.

This recruitment approach reflects both subtlety and ingenuity. The prospective agent was never confronted with a stark proposal to spy for the KGB, but was gradually drawn into such activity through apparent friendship and an ostensibly legitimate business arrangement. Similar techniques apparently were used by Gennadiy Zakharov, the Soviet physicist employed at the United Nations who was arrested on August 23, 1986, for buying classified documents from an FBI-controlled double agent whom he had attempted to recruit. See Appendix E for the indictment and an FBI affidavit filed in this case. The recruitment of William Bell, which also used a consulting ploy, is described in Appendix C. The finesse with which a good intelligence officer can draw a person into espionage is a strong argument for informing the FBI when one is approached by foreign officials, as this Report recommends later. Advice from counterintelligence experts can help to prevent tragedies.

Recruitment is more commonly accomplished on the basis of positive inducement than by coercive approaches such as blackmail, which are the last resort for the hostile intelligence service. Blackmail produces the least satisfactory, because least willing, sort of agent. But such methods are nonetheless used with some frequency when preferable methods fail or are unavailable. This is particularly true outside the United States, and especially in Communist countries where hostile intelligence services control the total environment. Entrapment through contrived circumstances can easily be arranged. Sexual entanglements, currency exchange violations and black market involvement are favorite recruitment ploys. U.S. diplomatic personnel, among others, have been targets of hostile intelligence services using these techniques.

Visitors with intelligence value are routinely approached by provocateurs with proposals of this kind, and ensuing arrests or threats of arrest or exposure serve as leverage for enlistment in espionage. For example, employees of U.S. firms with defense contracts who visit the Soviet Union or Eastern Europe will be given special attention and assessment for possible intelligence exploita-

tion. Visa applications reveal where an American works, and falsification of such information is itself an offense that can be used against an American visitor. Whether active recruitment is attempted depends upon whether the American provides indications of susceptibility to inducement or coercion. While travel to Eastern Europe is not, for the most part, discouraged, those who go can reduce their vulnerability by not doing or saying anything that could be recorded or photographed for future reference in the archives of the KGB.

In the final analysis, however, the most dangerous agents of all, who account for the greatest losses of the most highly classified information, are not those who are laboriously recruited, but those who walk in the door of a Soviet embassy somewhere and volunteer information for sale. For the "walk-in" as for the recruited agent, the motivating factors are usually greed or indebtedness plus an additional element of grievance or disgruntlement. The individual usually is dissatisfied with his or her job or harbors some grudge against his organization or both.

Some characteristic signs that may betray an agent at work, if security people and co-workers are sufficiently alert, include:

Attempts to obtain information when there is no need to know and excessive curiosity about what others are doing;

Unauthorized removal of classified material from work areas or introduction of cameras or recorders into work areas;

Repeated overtime or unusual work hours not required by the job; and

Unexplained affluence.

Indicators of espionage are, unfortunately, generally much more noticeable in retrospect than during the course of the crime. In many cases, it is difficult to distinguish the spy from an exceptionally hard worker. But suspicious activities such as those listed, combined with job dissatisfaction or other disgruntlement, would certainly provide grounds for heightened attention to an individual's actions. It was sensitivity to such behavior, after receiving a security awareness briefing in the wake of the Walker-Whitworth arrests, that led Jonathan Pollard's co-workers to alert the FBI, resulting in his arrest and conviction for espionage. This Report later recommends both improved security awareness programs and, in some areas, personnel reliability programs that incorporate peer-group cooperation.

5. Technology Transfer

The Soviet drive to achieve technological equality with the United States and other Western countries has led the USSR to commit enormous resources to the acquisition of open-source information, unclassified but proprietary information, and high-technology equipment that the West has agreed not to export to the Soviet bloc. Soviet intelligence services actively engage in these efforts in addition to their pursuit of U.S. secrets. As a result, the Western lead in many key technological areas has been reduced, with serious economic and military consequences for the United States.

Moscow has devised two programs to obtain Western technology. The first, under the Military Industrial Commission (VPK) of the Presidium of the Council of Ministers, seeks to obtain military and

dual-use hardware, blueprints, product samples and test equipment to improve the technical levels and performance of Soviet weapons and defense manufacturing equipment. By adapting design concepts from the acquired hardware and documents, the Soviets reduce their own research and development costs. In the early 1980s, more than 3,500 requirements were levied by the VPK each year, with about one-third being satisfied. Some 60 percent of the most significant acquisitions were of U.S. origin, although not necessarily collected in the United States. Nearly half of the up to 10,000 pieces of military hardware and 20 percent of the 100,000 engineering and research documents the USSR acquires annually worldwide are used by the Soviets to incorporate Western technology into their military research projects. Most of the documents, about 90 percent of which are unclassified, contain patented or copyrighted proprietary information and are illicitly obtained.

The GRU is believed to have satisfied considerably more VPK requirements than the KGB. This success is attributed partly to the GRU's greater scientific orientation and its wider variety of technology-related cover positions. The approximately 1,500 GRU officers serving outside the USSR have scientific and technological collection as an integral part of their responsibilities. The KGB S&T unit, Line X, has nearly 300 officers on foreign assignment operating under cover of Soviet embassies, trade and commercial organizations, as members of exchange groups, and as employees of international organizations (the United Nations Secretariat, for instance, as in the case of Gennadiy Zakharov).

The second program, managed by the Ministry of Foreign Trade and the KGB/GRU, seeks, through trade diversions, to acquire relatively large amounts of dual-use manufacturing and test equipment for direct use on production lines. This program attempts to obtain export-controlled microelectronic, computer, telecommunication, machine-tool, robotic, diagnostic and other sophisticated equipment. This program also utilizes both legal and illegal means.

Major Soviet collection efforts are targeted at microelectronics fabrication equipment and computers; nearly one-half of detected trade diversions fall into these categories. The acquisition of much of the information concerning these high-technology areas is not particularly difficult. Information is often available to the public (and, therefore, accessible to the Soviets and their surrogates) from U.S. Government agencies.

The Soviets and their allied intelligence services have for many years been regular attendees of scientific, technical and industrial conferences in the United States and abroad. The Soviets considered some of the information obtained from these conferences to be among the most significant contributions to their military projects. The VPK identifies those having the most potential; in recent years, these have included conferences assembled by several well-known professional engineering societies.

In addition, the Soviet Ministry of Foreign Trade and academic-related collectors contribute to Soviet exploitation of open-source Western information. The Ministry of Foreign Trade has hundreds of trade organizations and companies around the world. KGB and GRU officers operating under cover of these establishments collect large quantities of data openly, in addition to that derived from

64-268 O - 86 - 2

their covert operations. The Ministry, as an independent collector, helped meet about 15 percent of all fully satisfied VPK requirements during the late 1970s and early 1980s. It specializes in acquiring microelectronics, manufacturing equipment and communications dual-use products.

Equipment is obtained through the use of dummy firms, false end-user certificates and falsifications of export licenses by the Soviets and professional trade diverters whom they hire. Many advances in Soviet microelectronics have been made possible by the illegal acquisition of equipment from the West. The result, according to U.S. Government estimates, has been a marked reduction in the Western technological lead from about 10–12 years a decade ago to about half that today.

Richard Mueller, a West German citizen, has been involved in illegal technology acquisitions for the Soviets for more than a decade. Using dummy and front firms, he has diverted advanced computers and microelectronics equipment of significant value to the Soviets. Mueller was the moving force in the 1983 attempted diversion to the USSR of several Digital Equipment Corporation VAX super mini-computers that would have assisted the Soviets in computer-aided design applications for microelectronics fabrication.

6. Active Measures and Disinformation

"Active measures" and "disinformation" are terms for Soviet covert action operations designed to implement Soviet policy goals by attacking U.S. policy and by promoting a positive image of the Soviet Union. They are significant weapons in the Soviet strategy to discredit and deceive the United States and its allies. The Soviets' principal techniques include the use of front groups, agents of influence, media manipulation and forgeries. The nature and scope of Soviet "active measures" was spelled out in detail in published hearings before the House Permanent Select Committee on Intelligence in 1982 and before the Senate Foreign Relations Subcommittee on European Affairs in 1985.[4] Deputy Director of Central Intelligence John McMahon testified that the Soviets have a $3–4 billion program to influence public opinion in countries throughout the world. It combines all forms of overt propaganda and covert political action, including systematic disinformation efforts.

"Disinformation" is a convenient label to describe a variety of techniques. The classic example is forged documents used to discredit the United States or to supply proof of Soviet propaganda claims. Another method is to recruit and pay agents in foreign news media to slant their reporting and plant false stories. The Soviets also secretly fund and control front organizations and individual agents to promote pro-Soviet or anti-U.S. positions. The Soviets themselves use the term "active measures" to describe their covert disinformation and political influence operations.

---

[4] *Soviet Active Measures*, Hearings before the Permanent Select Committee on Intelligence, House of Representatives, July 13–14, 1982, U.S. Government Printing Office (Washington: 1982).

Soviet Active Measures, Hearing before the Subcommittee on European Affairs, Committee on Foreign Relations, United States Senate, September 12–13, 1985, U.S. Government Printing Office (Washington: 1985).

It is also fair to say that most overt Soviet propaganda is also a form of disinformation because of its systematic distortion of reality to advance Soviet interests. Whenever a prominent Soviet citizen addresses a foreign audience, his or her remarks are likely to reflect a calculated effort to influence the audience. The same is true of Soviet print and electronic media.

Every country tries to sell its viewpoint. What distinguishes the Soviet effort are the immense resources and systematic controls that are employed. Two organizations develop and implement the Soviet "active measures" strategy: (1) the International Department of the Communist Party of the Soviet Union, which coordinates foreign policy and propaganda objectives and now includes most of the work of the Party's former International Information Department; and (2) Service A of the KGB's First Chief Directorate, which conducts covert political influence and forgery operations. The CIA has estimated that if the United States were to undertake a campaign the size of the Soviet "neutron bomb campaign" of the 1970s, it would cost over $100 million.

Currently, there is evidence of a major Soviet active measures campaign against U.S. development of the Strategic Defense Initiative (SDI). The Soviets are making every effort to convince a world audience that SDI will destabilize an already precarious superpower armaments balance. In addition, Soviet active measures directed at U.S. allies, such as in West Germany and Japan, are designed to sow distrust of American policies and to intensify financial and commercial rivalries with the United States by holding out the promise of favorable terms to the business communities in both countries. Such techniques are more subtle than blatant forgeries, which may be less effective in furthering Soviet objectives in sophisticated Western countries.

Soviet active measures efforts are focused primarily on Third World countries. The Soviets appear to employ massive active measures currently in South Asia, in an effort to depict the United States as interfering in the affairs of India, Pakistan and Bangladesh. The media in all three countries have consistently carried stories to this effect. One long-running disinformation ploy concerns alleged attempts by CIA to aid separatist movements in India, thereby splitting the country, supposedly to America's economic advantage. Another frequent theme is accusations of CIA biological warefare efforts in the region. Discrediting U.S. intelligence agencies, particularly the CIA, has long been an important objective of Soviet active measures.

In some cases Soviet active measures directly involve domestic U.S. matters. During July, 1984, for example, the Soviets began a widespread disinformation campaign to discredit the Los Angeles Olympic Games and booster worldwide support for their boycott of them. This campaign featured three forged documents purportedly from racist groups, threatening Third World athletes with bodily harm if they participated in the Olympic Games. Shortly after their discovery, then-Attorney General William French Smith announced that the letters were KGB forgeries and part of a major Soviet disinformation effort. It has been determined that these documents fit the pattern of other Soviet forgery operations and were

part of the overall Soviet active measures campaign to discredit the Reagan administration and its handling of U.S.-USSR relations.

A very recent forgery sought to implicate the Chairman of this Committee. In August, 1986, U.S. news media received copies of a forged letter purportedly from an official of the United States Information Agency to Senator Dave Durenberger, purporting to discuss a proposed plan to exploit the Chernobyl nuclear power plant disaster for propaganda purposes. Analysis of the forged letter revealed that the letterhead and signature had been taken from a copy of an entirely different letter from the USIA official to the President of the Inter-American Defense Board. Ironically, the USIA official's letter had alerted the President of the Inter-American Defense Board to an earlier forged letter, in Spanish, purportedly from the Board President to Chilean President Pinochet. The circumstances of the earlier forgery indicated Cuban-Nicaraguan involvment. (See Appendix F for copies of the forged letters and the true letter.)

According to the CIA's 1982 assessment, it is sometimes hard to judge the success of Soviet active measures because they "tend to capitalize on and manipulate existing sentiments that are parallel to or promote Soviet foreign policy objectives. Whenever a political movement supports policies that coincide with the goals or objectives of Soviet foreign policy, the exact contribution of Soviet active measures to that movement is difficult to determine objectively." The CIA cites evidence that the Soviets themselves believe that their efforts are worthwhile. They appear to consider the "neutron bomb campaign" in Europe to be one of the most successful. On the other hand, the more recent campaign against Pershing and cruise missile deployment in Europe had much less impact. The FBI has described Soviet operations in the United States, moreover, as "often transparent and sometimes clumsily implemented." The FBI also states, "The American media is sophisticated, and generally recognizes Soviet influence attempts."

As noted later in this Report, the U.S. Government has stepped up efforts to expose Soviet disinformation and covert manipulation worldwide. The State Department now regularly publicizes the facts about Soviet forgeries and Soviet control of political organizations such as the World Peace Council, the Christian Peace Conference, and the 12th World Youth Festival.

The most sensitive aspect of the disinformation threat is Soviet deception of U.S. intelligence as part of an attempt to confuse or to manipulate the perceptions of U.S. policymakers. The Soviet military doctrine of *maskirovka* and the KGB concept of *dezinformatsiya* both emphasize the need for measures to mislead opposition intelligence services and to create false perceptions that will influence Western policy and undermine strategic capabilities.

The U.S. intelligence community recognizes the danger of deception and has a community-wide program to assess systematically the possibilities of successful Soviet efforts. The deception threat has been a focus of the Committee's oversight in recent years, and the Committee continues to support intelligence community efforts to maintain vigilance in this area.

One major means of countering any Soviet deception efforts is to leave our adversaries uncertain regarding the full extent of U.S. in-

telligence collection capabilities. Steps to maintain the security of U.S. human and technical intelligence capabilities make it much more difficult for the Soviets to engage confidently or successfully in deception efforts.

D. TECHNICAL COLLECTION OPERATIONS

Hostile intelligence services use the full range of intelligence-gathering technologies to collect sensitive information from the United States and our allies. Public discussion of technical collection methods is more difficult than the explanation of human intelligence techniques, because we do not want to tell the Soviets just how much we know about their operations. Countermeasures against technical threats work best when the hostile service does not recognize U.S. defenses and continues to conduct operations that can be substantially neutralized. At the same time, however, wider knowledge of the technical collection threat is essential to develop better security awareness and to explain the need for major resource investments. Technical threats include the interception of communications, other forms of electronic surveillance, collection of emanations from equipment, penetration of computer systems, and photoreconnaissance.

1. Interception of Communications

The interception of electronic communications and deciphering of machine-generated codes played a vital role in Allied intelligence during World War II—although the methods of collection were so sensitive that many aspects of these operations remained secret for thirty years after the war. An Anglo-American team of top mathematicians and cryptologists provided Allied commanders with vital realtime intelligence on German and Japanese intentions and plans. The interception of electronic communications and the computer-assisted assault on crytographic systems remains a central part of present-day signals intelligence.

The Soviet electronic monitoring effort represents a significant worldwide threat to U.S. military and civil telecommunications. This threat derives from large collection facilities that are operated in the Soviet Union, as well as in other countries around the world, such as Cuba. The Soviets also maintain a fleet of intelligence collection vessels that operate worldwide—including off both coasts of the United States. The latest of these vessels has been built from the keel up specifically for this role, unlike earlier ships that were reconfigured trawlers or other types of vessels. The Soviets also use merchant ships and possibly commercial aircraft to perform collection operations against targets of opportunity.

A serious threat is posed by the Soviet intelligence collection facility located at Lourdes near Havana, Cuba. Established in the mid 1960s, the site has steadily grown to its present size of about 2,000 technicians and is the most sophisticated collection facility outside the Soviet Union.

Evidence of the seriousness of the threat to electronic communications was emphasized by the issuance in 1984 of National Security Decision Directive No. 145, which concluded that "the compromise of U.S. information, especially to hostile intelligence services,

does serious damage to the United States and its national security interests."

The technology to exploit U.S. electronic communications is widespread, and many foreign countries use it extensively. Currently, more than half of all telephone calls in the United States made over any distance are vulnerable to interception. Calls that the caller believes to be on less vulnerable circuits may be automatically switched to more vulnerable ones. The Soviet diplomatic facilities at their Riverdale complex in New York City, at their consulate in San Francisco and at their new Mt. Alto embassy in Washington all occupy high ground, thus providing superior opportunities for communications intercept. The "Silicon Valley" concentration of high technology centers and the government's sensitive facilities in Washington and New York are at risk of intercept because of these Soviet sites.

It is especially important for civilian agencies and the private sector to understand the nature of the risk from Soviet interception of their communications. The Defense Department and the CIA have elaborate programs to inculcate communications security awareness and to protect classified communications links. The massive Soviet surveillance efforts from Cuba and elsewhere demonstrate, however, that the Soviet intelligence payoff from interception of unsecured communications is immense. One reason is that too many government officials and contractor employees discuss classified matters on unsecure lines because of the difficulty and expense of using currently available secure communications equipment. Another significant problem is the Soviet ability to exploit unclassified pieces of information that are relatively harmless in isolation, but in the aggregate provide highly damaging insights into U.S. capabilities. The Committee's classified Report contains several examples of how both industrial and national security can be harmed by such intercepts.

Public awareness of the hostile intelligence threat to domestic communications is essential, because there are real limits to what the U.S. Government can do to provide secure communications for the private sector. Although this Report later discusses some government initiatives, the protection must depend on the willingness of private organizations to invest in secure communications, not only for their immediate self-interest, but for the larger interests of the nation as a whole.

2. Other Forms of Electronic Surveillance

The Soviets have a long history of electronic attacks on the U.S. Embassy in Moscow, dating back to the 1950s when a replica of the Great Seal of the United States in the embassy was found to contain an audio device. In the late 1970s, a Soviet antenna was found in the chimney of the chancery. Additionally, Soviet and other hostile intelligence services try to gain access to office or communications equipment in order to "read our mail."

The vulnerability of the U.S. Embassy in Moscow was dramatized vividly by the recent discovery of the technical compromise of embassy typewriters. The typewriters were shipped to the Soviet Union by unaccompanied commercial means, thus affording the Soviets access to them. The compromised typewriters were used in

the embassy for a significant period. What made this incident especially astonishing was that it occurred despite a similar discovery in 1978, when security officers found that a shipment of IBM Selectric typewriters destined for the U.S. Embassy had been shipped from Antwerp to Moscow by a Soviet trucking line. The potentially compromised equipment identified in 1978 was returned to the United States before being placed in service. Unfortunately, the Soviets again gained access to several similar IBM machines that were not recognized for a substantial time as being compromised.

As noted earlier, foreign nationals with access to U.S. embassies and other establishments abroad provide a means for hostile intelligence services to make other electronic penetrations. Offices, residences and cars are all vulnerable to the planting of audio or video devices by foreign nationals with access, legitimate or otherwise, to the U.S. target.

Although all high technical threat U.S. diplomatic posts have eliminated the authorized access of foreign nationals to the vicinity of classified work areas, there remains a serious problem of common walls with uncontrolled adjacent areas from which technical attacks and even physical entries can be mounted. Offices and residences are also vulnerable to planted devices when access by foreign nationals is not properly monitored and technical countermeasures are not routinely employed.

In 1985, the Secretary of State's Advisory Panel on Overseas Security, chaired by Admiral Bobby R. Inman, provided to the Intelligence Committees of the House and Senate a classified annex to its report, covering, electronic and physical penetration of U.S. diplomatic facilities. The Inman Panel described the Soviet technical surveillance effort as "a technologically advanced and sophisticated program obviously supported by tremendous resources." The report went on to describe scores of discoveries of Soviet and Soviet-bloc technical exploitation of U.S. diplomatic premises. Noncommunist host nationals have also been detected mounting technical penetrations of U.S. missions.

The threat to office and communication equipment from the exploitation of unintended emissions is greater at U.S. facilities abroad than in the domestic environment, where the risks and costs of detection are considerably higher. Consequently, as noted by the Stilwell Commission on DoD Security Policies and Practices, the previously rigid requirements for expensive equipment shielding have been modified to prescribe shielding only when inspection verifies that a threat exists. There is, however, no question that such a potential threat does exist at especially sensitive locations in this country.

3. Penetration of Computer Systems

The hostile intelligence threat to U.S. computer systems is magnified by the enormous growth in the number and power of computers and the vast amount of data contained in them. The General Services Administration has estimated that the number of U.S. Government computers has increased from 22,000 in 1983 to over 100,000 in 1985. The increase in the number of computers in use in industry, business and other private sectors has been equally stag-

gering. Computers multiply enormously the information to which a single individual may obtain access.

There is a real possibility that the Soviets may exploit these vulnerabilities. Computers and computer software are high-priority items of both the VPK's and the Ministry of Foreign Trade's technology acquisition programs by legal or illegal means. The Soviet and other Warsaw Pact intelligence services have also obtained information concerning the methods used in the West to provide computer security, and constantly seek more knowledge. Over the past decade, the Soviets have acquired over 300 different types of U.S. and other Western computer hardware and software, which has enabled them to develop the technical ability to penetrate at least some U.S. automated systems. The Soviets are making a concerted effort to access state-of-the-art computers, including supercomputers.

The first Annual Report of the National Telecommunications and Information Systems Security Committee, completed in September, 1985, emphasized the challenge of computer security in both government and the private sector:

> Future technologies, particularly the growth of desktop computers, the increased local storage of data and the widespread networking, will exacerbate existing security vulnerabilities as well as create new ones. As this technology has grown, the resources and awareness needed to allow security technology to grow with it have not kept pace. The use of traditional COMSEC, physical security, personnel security, and administrative security protection techniques does not sufficiently protect the type of information-sharing that is becoming increasingly common in new automated information systems, especially distributed processing and networked systems.
>
> As storage costs decrease, the amount of data stored at the mainframes increases, creating more appealing targets. As the uses of networks and remote access expand, more and more users will have potential access to a broader range of information. As end-users of computers continue to increase their technical competence and computer literacy, the technical and management automated systems security task of protecting data and controlling users has fallen even further behind.

The NTISSC Annual Report admitted that "the full extent of the threat to and vulnerabilitis of automated information systems is unknown." Specific cases of unauthorized access to government computer systems have been detected and reported widely, including cases of access to and manipulation of Defense Department data in order to divert military equipment and weapons. There is no reason to believe that hostile intelligence services or their agents will ignore similar opportunities.

4. Imagery

The final category of technical intelligence collection is photographic or imagery intelligence—collection by means of overhead vehicles against adversary installations. The history of this disci-

pline dates to the use of observation balloons as platforms for photography during the Civil War and then use of aircraft for the same purpose during the two World Wars. The use of U-2 aircraft for imagery collection was extensively publicized in the 1960s. Today U.S. and Soviet imagery intelligence is collected primarily by satellite. The use of photographic satellites by both sides has gained wide recognition in the context of verification of compliance with arms control limitations.

Intelligence collection against the United States and U.S. interests worldwide using photographic means, or imagery, is carried out principally by the Soviet Union (with some assistance from its Warsaw Pact allies and Cuba). The Soviet imagery effort is mainly conducted from spaceborne and airborne platforms. The continued proliferation of Soviet satellites has given the USSR the concomitant capability for increased photoreconnaissance of its most obvious targets—U.S. and NATO strategic and tactical military forces, and crisis situations any place in the world. In addition to these uses of photoreconnaissance, the Soviets employ it to conduct earth resource surveys for economic and agricultural data.

Soviet spaceborne satellite reconnaissance capabilities are supported by the capability of military and civilian aircraft to collect photographic intelligence. The potential value of airborne reconnaissance conducted by the Soviet airline Aeroflot, which, in April, 1986, resumed operations to the United States, and by other Warsaw Pact national airlines' flights remains of concern. These Communist country overflights in the United States are under the jurisdiction of an FAA committee.

The Soviets continue to pursue intelligence-related manned space programs. In February, 1986, they launched a new type of modular space station, the MIR, replacing the older SALYUT-type modules. The MIR, as did the SALYUT, gives the Soviets the capability to perform a number of functions in space, including the use of cosmonauts to augment their other reconnaissance and surveillance efforts. The apparent military usefulness of their manned space program has been indicated in the Soviet announcement that "earth surface surveys" have been conducted; however, no photographs were ever published.

The seriousness of the imagery collection threat posed by Soviet and Bloc overflights in the NATO area can be illustrated by two examples. In March 1985, Norway banned or restricted Soviet and Bloc passenger airplanes from several airports on the basis that they were conducting electronic surveillance. Bulgarian aircraft were specifically mentioned as having departed from scheduled routes to overfly sensitive areas. In West Germany, some 1,500 Soviet Bloc overflights occurred in a three-month period in 1985, offering a tremendous opportunity for both electronic and photographic reconnaissance.

E. SUMMARY

Until the espionage arrests and disclosures of technical security compromises in 1985, the American people and most Government officials did not fully appreciate the magnitude and intensity of the hostile intelligence threat, despite previous espionage prosecutions

and knowledge of the vulnerability of U.S. communications to Soviet intercept operations. The barrage of revelations in 1985–86 has changed these perceptions, so that today there is a better recognition in Government and in the private sector of the continuing efforts by hostile intelligence services to collect sensitive information by human and technical means. There is also a greater awareness of Soviet efforts to influence the political process through "active measures" directed at countries throughout the world.

The Committee intends that this description and analysis of the hostile intelligence threat serve as a benchmark against which to measure further evolution of the threat in the years ahead and the effectiveness of counterintelligence and security programs. It is also important that the American people—especially responsible officials of private organizations in business and industry, science and technology, and international affairs—remain aware of the changing threat from foreign intelligence services. Such awareness does not mean exaggerating the dangers or engendering an atmosphere of suspicion. Rather, it is part of a mature understanding of the reality of U.S. relations with other countries in the world of competing national interests. The political and military rivalry between the Soviet bloc and the West is a fact of life that requires constant attention to ongoing and emerging Soviet bloc intelligence operations.

The hostile intelligence threat is, of course, only half the equation. On the other side are U.S. activities to counter this threat: counterintelligence, to uncover and to neutralize hostile intelligence activities; and security, to protect against both known and undiscovered hostile efforts by setting obstacles in the path of anyone seeking unauthorized access to sensitive information, activities, equipment or facilities. The rest of this Report examines the nature and effectiveness of those critical U.S. programs.

III. Counterintelligence

An effective response to the foreign intelligence threat requires a combination of counterintelligence and security measures. The Committee believes it is important to distinguish between counterintelligence efforts and security programs, while ensuring that both are part of a national policy framework that takes account of all aspects of the threat. The best way to explain the difference is to say that counterintelligence measures deal directly with foreign intelligence service activities, while security programs are the indirect defensive actions that minimize vulnerabilities. The FBI, CIA, and the counterintelligence components of the Defense Department have primary responsibility for operations and analysis dealing directly with foreign intelligence services. In addition, the Committee and the Executive branch have included within the national counterintelligence policy structure those diplomatic and regulatory policies that control the numbers and movements of particular countries' foreign intelligence service officers and co-opted agents in the United States and at U.S. facilities abroad.

A. NEED FOR A COUNTERINTELLIGENCE STRATEGY

By statute and executive order, counterintelligence functions are divided among the FBI, CIA, and components of the Defense Department. The FBI has the lead within the United States, while the CIA is in charge abroad. The Defense Department, which deals with threats to classified defense information worldwide, divides its counterintelligence functions among the military services, DIA, and NSA. No single official is responsible for the full range of counterintelligence activities below the level of the President and his National Security Adviser. Given these circumstances, there is a constant risk of fragmentation and conflict among organizations with different methods and priorities.

The Committee has found that communication and cooperation among U.S. counterintelligence agencies have improved greatly in recent years and are probably better today than at any time since World War II. Nevertheless, more needs to be done to ensure that agencies learn from each other's experiences and that progress achieved in one area can have benefits for others. The issue is not just communication and operational coordination to bridge jurisdictional boundaries. Better long-range planning is also needed to make optimal use of limited resources worldwide against well-organized and sophisticated adversaries.

Soviet bloc and PRC intelligence operations do not respect geographic boundaries. Thus, in many recent cases Americans who committed espionage in the United States met their foreign intelligence service contacts abroad. The targets and techniques needed for counterintelligence success transcend agency jurisdictions. For these and other reasons, the Chairman and Vice Chairman of the Committee stated in October, 1985, that the Executive branch should develop a national counterintelligence strategy that establishes national objectives and integrates the planning and resources of each agency to achieve these objectives. The President's interim report to the Intelligence Committees indicated agreement with this proposal, and in fact the Executive branch is now preparing such a document.

The organizational structure is already in place, fortunately, to develop a national counterintelligence strategy. Under the National Security Council, there is a Senior Interdepartmental Group for Intelligence (SIG–I) chaired by the Director of Central Intelligence. Within that framework, an Interagency Group for Counterintelligence (IG–CI), chaired by the FBI Director, develops national policy recommendations and provides a forum for agreement on new initiatives. A small secretariat for the IG–CI has expert personnel drawn from the FBI, CIA, and Defense Department. This staff evaluates the threat and recommends policy initiatives for counterintelligence and countermeasures improvements.

The IG–CI, assisted by its secretariat, is the proper place to develop a national counterintelligence strategy. This structure ensures joint participation by the FBI, CIA and Defense Department; and other interested departments and agencies (such as the State and Justice Departments) are also represented on the IG-CI. Ultimate responsibility for resolution of policy issues rests with the Na-

tional Security Council, which has recently brought onto its staff an experienced FBI counterintelligence specialist.

The President's interim report to the Intelligence Committees indicates that the IG-CI has, in fact, been tasked to frame strategic guidance of the sort proposed by this Committee. As noted earlier, member agencies are now engaged in the drafting process.

Findings and Recommendations

1. Findings.—The IG-CI has been chartered to frame national counterintelligence objectives and an associated strategy (or master plan) to further those objectives, and to submit the objectives and plan for consideration by the SIG–I and thence the NSC. The Committee is pleased to learn that Executive branch agencies are actively drafting this document. This is a positive response to proposals presented by the Chairman and Vice Chairman in testimony before the Permanent Subcommittee on Investigations in October, 1985.

2. Recommendation.—The National Security Council should approve a statement of major counterintelligence objectives and a strategy, i.e., a time-phased master plan, to attain those objectives. The House and Senate Intelligence Committees should receive this document. An effective oversight mechanism should be established to ensure that major programs and associated budgets, legislative proposals, and other key actions are validated against the master plan, constitute judicious and operationally efficient allocation of resources, and achieve all feasible synergism. There should also be a process for continuing review and evaluation.

3. Recommendation.—The National Foreign Intelligence Program should provide for, and Congress should authorize, augmentation of the staff that assists the IG–CI to ensure effective performance of its expanded responsibilities regarding the development and implementation of the national counterintelligence strategy.

B. HOSTILE PRESENCE LIMITS

An effective national counterintelligence strategy should include diplomatic and regulatory policies that control the numbers and movements of hostile intelligence service officers and co-opted agents in the United States and at U.S. facilities abroad. Each year, in the formal classified justification for funds for its Foreign Counterintelligence Program, the FBI advises Congress that, even with increased resources, the FBI cannot cope with the hostile intelligence threat unless measures are also taken to reduce the number of potential intelligence officers in this country. Where the numbers cannot be reduced, controls on their movements can assist the FBI in making better use of limited resources.

The Foreign Missions Act of 1982, which created a new Office of Foreign Missions in the State Department, provided the authority to exercise greater control over the activities of foreign officials in this country. Although such control is normally exercised within the framework of diplomatic reciprocity, the Act also facilitates actions to enhance U.S. security and counterintelligence interests. Limits on numbers of foreign representatives allowed into the United States are usually left to Executive branch discretion, but

the Leahy-Cohen amendment in 1985 established a policy of equivalence between the number of Soviet embassy and consular personnel in the United States and the number of U.S. embassy and consular personnel in the Soviet Union. The 1985 Roth amendment provided for regulation of travel by U.N. Secretariat personnel from countries whose diplomats are subject to such regulations under the Foreign Missions Act.

National Security Decision Directive (NSDD) 196, signed by the President on November 1, 1985, established national policy objectives for restricting and controlling the hostile intelligence presence and travel in the United States. In addition to implementing the Leahy-Cohen and Roth amendments, the Administration has imposed Foreign Missions Act travel regulations on representatives of Warsaw Pact countries whose intelligence services act as Soviet surrogates, has begun reducing the number of Soviet representatives in the United States, and has supported extension of Foreign Missions Act controls to commercial and other entities used by hostile intelligence services in this country. Consistent with these Presidential objectives, Committee Members introduced legislation to establish a policy of equivalence for the size of the U.S. and Soviet Missions to the United Nations (Leahy-Cohen), to broaden the scope of the Foreign Missions Act to cover commercial and other entities controlled by foreign governments (Durenberger-Leahy), to require registration by commercial entities controlled by Warsaw Pact governments (Roth-Nunn), and to require imposition of Foreign Missions Act travel regulations on representatives of Warsaw Pact countries (Roth-Nunn).

The 1985 Roth amendment has been implemented by imposing travel restrictions on U.N Secretariat representatives/employees from the Soviet Union, Afghanistan, Vietnam, Libya, Iran and Cuba. The State Department's Office of Foreign Missions Travel Bureau Service has been required for use by U.N. Secretariat personnel from East Germany, Czechoslovakia, Bulgaria, and Poland. Most recently, it was publicly announced that effective October 1, 1986, the Soviet Missions to the United Nations will be required gradually to decrease their size from 275 to 170, to be accomplished by April, 1988.

In 1986, the Committee received three reports on Executive branch efforts to control the hostile intelligence presence. The first was a report on the respective numbers and treatment of officials from countries that conduct intelligence activities in the United States contrary to U.S. interests and the numbers and treatment of U.S. officials in those countries. Under the Leahy-Huddleston amendment of 1984, this requirement covers the Soviet bloc, Cuba, China, and any other nation designated on the basis of the threat posed by its intelligence or terrorist activities. The second was a report from the Secretary of State and the Attorney General on plans for implementation of the policy of substantial equivalence between U.S. and Soviet embassy and consular personnel pursuant to the Leahy-Cohen amendment of 1985. The third was the annual report of the State Department's Office of Foreign Missions, which regulates many aspects of the treatment of foreign government establishments and officials in the United States.

These reports reflect uneven progress in limiting the hostile intelligence presence in the United States. While the planned reduction in the size of the Soviet U.N. mission is an important step forward, the intent of the Committee in recommending the Leahy-Cohen amendment was also to reduce the number of Soviet embassy and consular personnel in the United States. The plan for implementation of diplomatic equivalence does not achieve that objective. Instead, there is a potential for actually increasing the number of Soviet embassy and consular personnel in the United States if the State Department carries out its plan for a Soviet consulate in New York and permitting a U.S. consulate in Kiev. According to the plan received by the Committee, the number of Soviet diplomatic and consular officials will increase from 320 to as many as 350, depending on the number of Americans sent to Kiev. Current plans call for thirty U.S. officials in Kiev. Apart from the merits of the need for so large an establishment in Kiev, the Committee believes that at a minimum the Soviets should be required to staff their New York consulate within the 320 ceiling on overall representation in the United States. The State Department should plan accordingly to staff the U.S. embassy and consulates in the Soviet Union within a comparable 320 ceiling.

The Committee supports the State Department's plan to reduce the Soviet work force at the U.S. Embassy in Moscow. This plan would also allow the staffing of a small consulate in Kiev within the 320 ceiling and still permit some reduction in Soviet embassy and consular positions in the United States. Such reductions could be made, for example, by refusing to allow the Soviets to replace officials expelled from the United States for espionage-related activity. Further reductions should be possible as the Americans who replace Soviet employees learn to do their jobs more efficiently.

Apart from issues of numerical equivalence, the State Department through the Office of Foreign Missions has made considerable progress in imposing more effective controls. In addition to regulating the travel of Soviet bloc representatives and U.N. Secretariat personnel, the Office of Foreign Missions (OFM) is requiring Soviet bloc embassies to secure prior OFM approval of purchases or leases of property for housing as well as business purposes. A Soviet request to construct a new apartment building in their existing compound in Riverdale, New York, has been denied because it is deemed excessive to Soviet housing needs. On May 28, 1985, the Soviets were advised that their procurement within the United States of building equipment, materials, or services for the remaining construction work at their Mt. Alto site in Washington, D.C., must be arranged through OFM. In response to a Soviet request to expand its recreational facilities at Pioneer Point, Maryland, OFM has told the Soviets they must abide by the same terms and conditions applied to construction on the site of U.S. Embassy recreational property in Moscow.

The Committee believes the OFM program is one of the most important recent counterintelligence initiatives, and is recommending legislation to broaden OFM's authority to impose travel controls on certain Soviet bloc-controlled businesses located in the United States. The Committee also supports OFM's plans to require Soviet bloc missions to lease residential units from OFM, to purchase tele-

communications goods and services through OFM, and to use OFM banking services. OFM's effectiveness will be enhanced by the Administration's decision to give Ambassador status to its current Director. (By law, his successor will have such status.) The Committee supports the decision to make this appointment, so as to strengthen the Director's ability to deal with foreign representatives.

The need to combat the hostile intelligence presence must also be taken into account in developing policies and regulations for exchange programs. There is clear evidence that some exchange visitors are used for clandestine intelligence purposes. While foreign policy considerations may dictate greater openness between the United States and certain countries, they must be balanced against the counterintelligence risks. The President's interim report to the Intelligence Committees states that efforts are made to do this.

Overseas, the hostile presence problem has three separate dimensions. The first is employment of Foreign Service Nationals (FSNs) at U.S. diplomatic missions. While most attention has been focused on the large number of Soviet nationals employed at our Embassy in Moscow, similar concerns arise in other countries. The Inman Panel on Overseas Security recommended reducing the number of FSNs at embassies in other Warsaw Pact countries and segregating them from sensitive areas and positions in other missions. The State Department has developed a plan to reduce the number of FSNs in Moscow to 95 and to begin such reductions elsewhere.

The Committee supports both the Moscow effort and the modest FSN reductions planned in Eastern Europe. The Administration requested $6.3 million for FY 1986 and $28.3 million for FY 1987 to meet the costs of such staffing changes; the urgent supplemental appropriations bill met $12.0 million of that need. The Committee urges the State Department to reprogram the remaining needed funds, especially if construction funds appropriated in the urgent supplemental cannot be fully expended in FY 1987.

A second aspect of the problem is the employment of over 120,000 foreign nationals at U.S. military installations. Close to 1,000 of these personnel have access to some classified information; roughly 370 have access to some Secret material. The Stilwell Commission recommended stricter personnel security safeguards in such cases, and consideration should also be given to reducing the military's reliance on foreign nationals, who are much more likely to be recruited by a foreign intelligence service than are U.S. personnel. The Committee recognizes that status of forces agreements limit the hiring of U.S. citizens to perform unclassified work at overseas bases, but the number of foreign national employees with authorized or unauthorized access to classified information can and should be reduced to the minimum feasible level. The Committee supports the tighter investigation requirements for foreign employees that have been recommended by the Stilwell Commission.

The State Department plays a key role in developing and implementing these policies and in ensuring that they take into account other U.S. foreign policy objectives. Components of the State Department vary in their understanding and appreciation of counterintelligence concerns. It is important to provide better training and other information on the foreign intelligence threat to State Department officials. While the State Department is not a counterin-

telligence agency, its officials should be kept fully apprised of the threat so they can be better prepared to support Foreign Missions Office and other policies designed to implement a national counterintelligence strategy.

Findings and Recommendations

4. Recommendation.—Recent Administration initiatives and legislation (Leahy-Cohen amendment, Roth amendment) should be implemented in a manner that places effective limitations on the numbers and activities of hostile intelligence service personnel in the United States and takes into account our foreign policy and intelligence collection efforts. The limit of 320 on permanently accredited. Soviet embassy and consular personnel should not be increased, and the State Department should plan to staff the U.S. embassy and consulates in the Soviet Union so as to require some reduction in Soviet embassy and consular personnel in the United States.

5. Recommendation.—Congress should enact legislation establishing a policy of substantial equivalence between the size of the Soviet and U.S. missions to the United Nations in line with the Administration's plan to reduce the size of the Soviet U.N. Mission.

6. Recommendation.—Congress should strengthen the authority of the Office of Foreign Missions to regulate commercial and other entities controlled by foreign governments and require registration of commercial entities controlled by Warsaw Pact governments.

7. Recommendation.—The Committee supports efforts through the Office of Foreign Missions to enhance U.S. counterintelligence effectiveness, including new initiatives to require Soviet bloc missions to acquire residential property, telecommunications services and equipment, and banking services through OFM. The Committee also supports the granting of Ambassador status to the current OFM Director.

8. Recommendation.—Policies and regulations for exchange programs with other countries should take counterintelligence concerns into account.

9. Recommendation.—The State Department should reprogram whatever funds are needed to supplement the $12.0 million appropriated through FY 1987 to implement plans to replace a substantial number of Foreign Service Nationals with Americans at U.S. missions in the Soviet Union and other high-risk countries. The Defense Department should reduce the use of foreign nationals with access to classified information at DoD installations abroad, and Congress should appropriate sufficient funds to replace them with Americans. Funds for this purpose should be requested in the FY 1988 budget, and DoD should determine what changes may be required in mandated military ceilings overseas.

10. Finding.—In conjunction with the CIA, FBI and DoD counterintelligence components, the State Department should have a program of formal training sessions, briefings and intelligence reporting arrangements to provide more and better information to State Department officials on the foreign intelligence threat and U.S. counterintelligence requirements. The Committee notes with pleasure that progress is being made in this area.

C. COUNTERINTELLIGENCE AWARENESS PROGRAMS

One key to a successful counterintelligence strategy is thorough analysis of the hostile intelligence threat and communication of the results to those who need to take countermeasures. Current efforts range from the FBI's Development of Counterintelligence Awareness (DECA) program for briefing defense contractors to the improved assessment of Soviet deception, disinformation and active measures. Informing the public, industry and other government agencies can have a direct payoff, as in the case where a student at Columbia University contacted the FBI about a Bulgarian exchange visitor after seeing a TV documentary on espionage that described conduct similar to that of the Bulgarian. The student's report led to an FBI offensive double agent operation resulting in the arrest of a Bulgarian intelligence officer. At a classified level, U.S. counterintelligence agencies must work with a great variety of government programs and security officials to provide tailored information and analysis.

On November 1, 1985, the President issued NSDD-197 requiring each U.S. Government agency to establish a security awareness program for its employees, including periodic formal briefings on the threat posed by hostile intelligence services, and to provide for the reporting of employee contacts with nationals of certain foreign powers. These programs are to be tailored to the sensitivities of particular work and designed so as not to intrude into employees' privacy or freedom of association.

According to the NSC staff, department and agency heads have responded positively and have given high priority to this enterprise. The State Department contact reporting directive, which has been provided to the Committee, serves as a good model because it specifies reporting procedures clearly and identifies those countries that require the greatest attention. Civilian agencies without extensive national security responsibilities also appear to be taking this policy initiative seriously.

The Committee strongly supports this policy and is recommending that a similar security awareness program be established for the U.S. Senate. The Committee has used the State Department's new program as its model.

The Larry Wu-tai Chin case highlighted the threat posed by Chinese intelligence operations. As indicated in section II of this Report, however, the PRC intelligence threat differs greatly from the Soviet one. These differences require development of new counterintelligence approaches geared to the special characteristics of the PRC threat. In particular, the FBI should develop specialized threat awareness briefings geared to the unique problems posed by PRC operations. At the same time, FBI threat awareness programs do not—and should not—leave the implication that lawful association with or assistance to Chinese technical and scientific researchers is a sign of disloyalty to the United States.

Another aspect of counterintelligence awareness is the knowledge by agency security officials of when to bring a matter to the attention of a U.S. counterintelligence agency. In the Edward Lee Howard case, CIA security officials failed to alert and involve the FBI in a timely fashion. The CIA has taken steps recently to guard

against a recurrence of this problem. The FBI should continue to work closely with security officials of all U.S. Government agencies to ensure that they understand its requirements and guidelines. A good example is the Pollard case, where the Naval Investigative Service Command brought in the FBI at an early stage. The Committee is pleased that the Navy has given a commendation and a monetary award to the official who was responsible for bringing the FBI into the Pollard case promptly when certain questionable behavior was observed.

The lessons of the Howard and Pollard cases should be extended to all departments and agencies that handle highly sensitive information. Interagency procedures for reporting suspicious conduct to the FBI should be strengthened. Moreover, the Howard and Pelton cases demonstrate that former employees with grievances or financial problems can compromise our most sensitive national security programs. Individuals who choose to work in positions as sensitive as those occupied by a Howard or a Pelton should expect to be held to a higher security obligation than personnel with access to less sensitive information. Therefore, the FBI should be informed when employees with access to extremely sensitive information resign or are dismissed under circumstances indicating potential motivations for espionage. The decision as to whether the circumstances justify investigation in varying degrees should be made by the FBI, in light of its counterintelligence experience, not by the employing agency. Interagency procedures should be established to address borderline cases.

Threat analysis functions are shared among U.S. counterintelligence, foreign intelligence and security agencies. Development of an effective national counterintelligence strategy, as well as a comprehensive and balanced set of security measures, requires centralized assessment of the threat posed by all forms of collection—technical as well as human. Since 1981, an interagency staff has compiled assessments of the hostile intelligence services threat and U.S. countermeasures, based on inputs from throughout the Government. The Committee has found these assessments to be increasingly valuable and is pleased that they continue to have high priority.

National assessments are no substitute, however, for high-quality threat assessments tailored to meet more specific needs. The Committee is pleased to learn that progress is being made regarding one such need for tailored material that was highlighted in the most recent interagency assessment.

DoD counterintelligence agencies have taken the lead in analyzing the threat to particular military installations and activities. The Committee supports increased efforts in this area, especially to assess the threat to highly sensitive research and development projects and to make the findings available to the officials responsible for security countermeasures. In recognition of the importance of this function, the Stilwell Commission has recommended, and the Secretary of Defense has directed, that the Defense Intelligence Agency establish a Multidisciplinary Counterintelligence Analysis Center as a service of common concern for DoD to meet the counterintelligence analytic requirements of the Defense Counterintelligence Board and the various DoD components. DIA should have

the task of ensuring that other agencies' threat assessments are responsive to security and program management needs of DoD components. Efficient allocation of limited security resources depends on careful evaluation of the threat.

Special attention is required for two aspects of the hostile intelligence threat that directly relate to U.S. foreign intelligence analysis: deception; and "active measures," including disinformation, forgeries and other political influence operations. Hostile intelligence services conduct these operations in addition to their collection efforts.

An interagency committee and a community-wide intelligence analysis office are both active in the analysis of deception efforts. Pursuant to the Committee's classified reports accompanying the Intelligence Authorization Acts for FY 1985 and FY 1986, a small interagency staff has been assigned to the analysis office.

In recent years, with the help of the intelligence community, the State Department has stepped up efforts to expose Soviet "active measures," such as forgeries and Soviet control of political organizations and conferences abroad. The Committee supports recent initiatives to improve intelligence support for U.S. efforts to counter these Soviet activities.

The State Department and other appropriate agencies should do more to disseminate the results of such analyses to opinion leaders and policymakers worldwide. Recent steps to increase the effectiveness of the Active Measures Working Group, which is chaired by State/INR, are welcomed by the Committee. The Working Group has briefed U.S. embassies on its role, encouraged the formation of embassy committees to monitor and combat Soviet active measures, and arranged for both classified and unclassified guidance to be provided to the field on specific cases. These efforts should be supported and fully staffed by the relevant agencies, especially the State Department. The Committee is pleased that a new office has been established recently in State/INR for this purpose.

The FBI prepares reports and testifies before Congress on efforts in the United States by the Soviets and other designated countries to influence public opinion and government policy through "front" organizations and other covert operations. For example, in 1986 the Committee received a classified FBI report on "Trends and Developments in Soviet Active Measures in the United States," which updated a previous study prepared in 1982. The FBI report reviews covert Soviet political influence operations directed at U.S. public opinion and policymakers. The Committee regularly requests further counterintelligence information from the FBI on such operations. The Bureau should continue to report these assessments in a manner that provides the necessary facts about hostile intelligence activities and that fully respects First Amendment rights.

Findings and Recommendations

11. Recommendation.—All elements of the U.S. Government should give high priority to implementation of the policy requiring security awareness briefings and the reporting of contacts with nationals of designated countries. A similar procedure should be adopted for U.S. Senate personnel.

12. Recommendation.—The Howard case demonstrates the need for strengthening interagency procedures for bringing possible espionage cases to the FBI's attention in a timely manner. The FBI should also be informed when employees with access to extremely sensitive information, such as Howard and Pelton, resign or are dismissed under circumstances indicating potential motivations for espionage.

13. Recommendation.—The FBI should develop threat awareness briefings tailored to the special characteristics of the PRC espionage threat. Such briefings should alert American citizens to the risks of giving assistance to PRC nationals who may have espionage assignments, while respecting the freedom to associate with lawful scientific and technical research.

14. Finding.—Significant efforts are underway to improve counterintelligence threat analysis, including publication of regular interagency assessments of the hostile intelligence services threat and U.S. countermeasures and the establishment in DIA of a Multidisciplinary CI Analysis Center to meet DoD threat analysis requirements in conjunction with other DoD components. The Committee is also pleased to note that there has been progress in the effort to provide tailored analyses of the hostile intelligence threat.

15. Recommendation.—The relevant interagency intelligence analysis office should coordinate and sponsor analytic efforts on Soviet deception, disinformation and active measures. The State Department and other agencies should increase dissemination of information about Soviet active measures abroad. The FBI should continue to be responsible for reports on active measures in the United States by hostile intelligence services and should cooperate with interagency analytic efforts. Reports on active measures in the United States that are prepared by agencies other than the FBI should be prepared in coordination with the FBI and/or the Attorney General.

D. DOMESTIC OPERATIONS

Counterintelligence operations in the United States differ from such operations abroad, because the environment is generally more favorable. U.S. counterintelligence has greater resources, easier access to the target, and public attitudes favorable to citizen cooperation. While legal requirements place constraints on surveillance techniques and investigative methods, those limits are vital for maintaining our free society and (with exceptions discussed below) do not inhibit necessary counterintelligence efforts.

Domestic operations can be divided into the following categories: surveillance coverage of foreign government establishments and officials; offensive operations to recruit agents-in-place and defectors or to control double agents; and espionage investigations and prosecutions. Many of the strategic requirements for domestic operations are unique, especially with respect to surveillance of establishments and officials and the investigation and prosecution of espionage cases. Other requirements have more in common with overseas operations, particularly with regard to penetration of hostile services, handling of defectors and double agents, and analysis of the *bona fides* of sources. Unique features of overseas operations,

as well as personnel management and training programs that cross geographic divisions, are treated in later sections of this Report.

1. Coverage of Establishments and Officers

The foundation for domestic counterintelligence is systematic collection on a foreign country's official representatives in the United States. Such collection may be technical or human.

Recent cases have shown the vital importance of comprehensive coverage of Soviet bloc embassies and consulates as a means of detecting offers to sell U.S. secrets. Pelton, Cavanagh, Jeffries and others made their initial contacts with the Soviets by contacting an establishment. Skilled counterintelligence work is required in such cases, and frustrations may be unavoidable. The Pelton case is an example in which it took years to achieve a positive identification.

The stratgegic importance of covering certain foreign establishments and their employees justifies continuing resource investments to upgrade the FBI's surveillance capabilities. The Committee has supported such investments over the years and continues to do so.

In this connection, the importance of the contact reports discussed earlier in this Report cannot be overemphasized. While government regulations can require federal employees to report contacts with possible foreign intelligence officers, a free society must rely on the voluntary cooperation of private citizens to advise the FBI of approaches and other contacts by such officials. Frequently the FBI requests citizens to report this information about particular individuals, based on surveillance of a contact. The FBI's DECA briefings, which are designed to encourage such contact reports from defense contractors and their employees, have now reached over 15,000 contractor employees. FBI and other intelligence community officials have used speeches and public appearances to emphasize the importance of public cooperation.

The American people have a legitimate concern that their government should not intrude upon their lawful associations with foreign officials and their First Amendment right to exchange ideas with visitors from abroad. For that reason, the FBI operates under guidelines established by the Attorney General and internal FBI policies overseen by the Committee that are designed to respect the free exercise of constitutional rights. As Director Webster stated in a recent speech:

> We certainly don't have enough Agents to keep track of every citizen of this country nor do we want to investigate the activities of lawful organizations without predication for doing so. Rather, our focus—indeed our strategy—must be on the intelligence operatives themselves and the identification of those who have come here with intelligence commissions. By building a spiderweb throughout the United States that focuses on them rather than on our own citizens, we make it much more difficult for those who would betray our country by surreptitiously supplying national secrets to foreign intelligence officers. I believe that in a free society this is the only way we can function without turning ourselves into a police state.

The existence of those safeguards should give the public confidence that cooperation with FBI counterintelligence not only serves the national interest, but is consistent with respect for constitutional rights.

Findings and Recommendations

16. Recommendation.—Congress should continue to fund increases in FBI surveillance capabilities.

17. Recommendation.—American citizens in all walks of life should be encouraged to assist U.S. counterintelligence efforts by providing information to the FBI, either upon request or when they are approached by possible foreign intelligence officers.

2. Offensive Operations

A major element in counterintelligence is offensive operations, especially efforts to recruit agents-in-place within hostile intelligence services and to induce defections from those services. The strategic payoff of agents and defectors can be immense, as demonstrated by the exposure of Edward Lee Howard and the successful prosecution of Ronald Pelton.

The greatest area of concern is the handling of defectors, as dramatized by the Yurchenko case. According to a CIA survey, most of the defectors resettled in the United States with CIA assistance are basically satisfied with their treatment. Nevertheless, a significant minority have problems that require special attention on a continuing basis.

In the aftermath of the Yurchenko re-defection, the CIA has undertaken a comprehensive review of its practices for handling defectors. Deputy Director of Central Intelligence Robert M. Gates summarized the CIA's conclusions and corrective actions at his confirmation hearing on April 10, 1986:

> There were organizational deficiencies. We have made organizational changes so that a single individual and a single organization are accountable and are in charge of the entire process for defectors. Another element that we have changed . . . is to ensure that the same person is basically the principal case officer for a defector with continuity, so that a defector isn't facing a whole new set of people all the time and there is somebody there that he gets to know and that he can depend upon and that understands him and understands his concerns, and can identify when he is going through a particular psychological crisis. . . .

Mr. Gates also called it "imperative" to assign individuals who speak the same language as a defector so that someone is available to talk in his or her own language; he did not know, however, whether the CIA has actually been able to implement this approach.

The actions taken and under consideration by the CIA reflect a constructive effort to upgrade the defector program and respond to the lessons of the Yurchenko case. They need continuing high-level support, both in the CIA and in other agencies. The Committee will

continue to assess the CIA improvements along with other approaches.

The Executive branch continues to examine the broad question of how defectors might best be welcomed, assisted and utilized. A private organization formed to assist defectors, the Jamestown Foundation, has recommended major changes in the defector handling program. The Committee intends to follow this issue closely in the coming year and looks forward with great interest to seeing the results of Executive branch deliberations.

The Committee considers it of the utmost importance that our nation's goals in welcoming and assisting defectors be more clearly enunciated and boldly implemented. Too often, the only operative goals have been the national security benefits that result from debriefing a defector; the defector's personal security against attacks by his or her country's security services; and enabling the defector to survive without continuing U.S. Government intervention. Other goals must be added to that list: to encourage achievement in American society consonant with the defector's talents and accomplishments; and to assist the defector in making a continuing contribution to the United States. While the Executive branch has taken steps to administer its current defector program more effectively, it must also effect this important change in attitude and commitment.

The Permanent Subcommittee on Investigations of the Senate Committee on Governmental Affairs has begun a major study of the U.S. Government's handling of defectors and other refugees from the Soviet Bloc. This study will focus particular attention on the contributions that defectors can and do make to American society and on the need to encourage that process. The Intelligence Committee supports this PSI study and is cooperating with the Subcommittee in its effort to inform the public regarding the needs of defectors and of the agencies that assist them.

Perhaps the greatest risk in a strategy of penetrating hostile services is that the agent-in-place or defector may be a double agent, pretending to be recruited by or escaping to the United States but actually controlled by a hostile counterintelligence service. Disputes over the *bona fides* of sources have plagued the U.S. intelligence community in the past. Such differences are sometimes unavoidable, but they should not disrupt interagency cooperation. Counterintelligence is not an exact science. The important thing is not to rely on a single source without careful testing and corroboration of his information. In this regard, the Committee has sought and received assurances that intelligence officials are alert to the risk of over-reliance on the polygraph.

The FBI, CIA, and DoD counterintelligence components have made extensive use of double agents, as evidenced in the recent Izmaylov and Zakharov cases. Last June, the Soviet air attache, Col. Vladimir Izmaylov, was expelled after being apprehended by the FBI. On August 23, Gennadiy Zakharov, a Soviet physicist working for the United Nations, was arrested and charged with espionage. Both Soviets had been maintaining clandestine contact with individuals who were cooperating with the FBI.

There is a clear need for these operations to be carefully managed. Counterintelligence managers must also review operations to

ensure that they have not been compromised. The Committee found Executive branch officials sensitive to these and other issues raised by double-agent operations.

The most difficult counterintelligence task is countering the use of "illegals," that is, hostile intelligence service officers who operate under deep cover rather than official cover. Some "illegals" may be used primarily for performing espionage support functions (e.g., clearing drops). The FBI and the Justice Department should consider improved ways to prosecute "illegals" for such espionage support activity.

Findings and Recommendations

18. Finding.—In the aftermath of the Yurchenko re-defection, the CIA has made improvements in its procedures for handling defectors. The Committee will continue to review the implementation of those procedures to ensure that needed resources and personnel, as well as continuing high-level support, are provided. The Administration has commissioned an independent assessment of the CIA defector resettlement program, and the results will be provided to the Committee.

19. Recommendation.—Objectives for the defector resettlement program must include encouraging the fullest possible achievement in American society and assisting defectors to make a continuing contribution to the United States. The Committee strongly supports the efforts of the Permanent Subcommittee on Investigations of the Senate Governmental Affairs Committee to focus public attention on the contributions that defectors can make to American society and on the need to enhance their ability to make such contributions.

20. Finding.—The Executive branch has reassured the Committee regarding the risk of over-reliance on the polygraph in testing sources and defectors and has demonstrated sensitivity to issues concerning the mangement of U.S.-controlled double-agent operations.

21. Recommendation.—The Justice Department and the FBI should work together to develop improved ways to prosecute "illegals" who perform espionage support functions. If further legislation is needed, the Justice Department should so inform the Congress.

3. Espionage Investigations and Prosecutions

Espionage investigations that may lead to criminal prosecution raise delicate issues of interagency cooperation and balancing of interests. Some senior officials support impostition of the most severe penalties on an individual found to have engaged in espionage on behalf of a hostile foreign power. Law enforcement objectives may conflict, however, with counterintelligence requirements and other national security interests.

Espionage cases involving non-Soviet bloc countries raise foreign policy issues, because of the desire of the United States to maintain good relations with particular governments. In the recent Pollard and Chin cases, however, the Executive branch has demonstrated its willingness and ability to investigate and prosecute espionage by agents acting on behalf of friendly countries—in these cases,

Israel and China. The Committee fully supports enforcement of the espionage laws, without regard to the foreign country involved. This policy does not necessarily conflict with other U.S. objectives requiring good relations with such countries, so long as it is applied even-handedly. The United States should make clear to every country that it will not tolerate violation of our espionage laws and that it will investigate the intelligence operations of countries that control or permit the commission of espionage in or against the United States on their behalf. The Committee is pleased with recent assurances of State Department cooperation with enforcement action whenever evidence of espionage is presented.

For many years U.S. counterintelligence officials assumed that information acquired by intelligence techniques could not be used for law enforcement purposes because of legal obstacles and the need to protect sources and methods. The Foreign Intelligence Surveillance Act and the Classified Information Procedures Act have made espionage prosecutions somewhat easier, although other difficulties still remain. These problems include the use of certain investigative techniques, the need for more expertise in handling sensitive espionage matters, and requirements for better cooperation among and within agencies.

One of the principal differences between espionage investigations and other criminal cases is the overriding need for secrecy to protect counterintelligence sources and methods. That is why Presidents have asserted claims of "inherent constitutional power" to authorize the use of intrusive techniques with Attorney General approval rather than a judicial warrant. That is also why Congress has established a special secure court order procedure under the Foreign Intelligence Surveillence Act and exempted counterintelligence from the law enforcement procedures for access to bank records in the Right to Financial Privacy Act. U.S. counterintelligence officials have consistently contended that ordinary judicial procedures do not provide adequate security in dealing with hostile intelligence services. In normal criminal cases the objective—either immediate or long-term—is always prosecution in open court. Counterintelligence operations have other objectives that may be more strategically important, such as learning the methods of the hostile service.

Federal law does not adequately take account of such differences in several areas. The FBI has found that the counterintelligence exemption in the Right to Financial Privacy Act is insufficient to obtain access to bank records when financial institutions refuse to cooperate on a voluntary basis. Consequently, the FBI is requesting legislation to give U.S. intelligence agencies the authority to require financial institutions to provide access to records. Unlike the law enforcement procedures under the Right to Financial Privacy Act, neither a court order nor notice to the subject of the records would be required. The FBI has a strong case for replacing the current voluntary system with a law that provides mandatory access for counterintelligence purposes within a framework of Attorney General guidelines and congressional oversight to provide safeguards against abuses. The Committee, therefore, has included legislation to address this need in the Intelligence Authorization Act for Fiscal Year 1987.

There is a similar problem with access to telephone and other telecommunications records. Paradoxically, it is easier in some states to wiretap an individual than to get the phone company to provide access to his or her billing records. For security reasons, the law enforcement alternative of a grand jury subpoena is usually impractical; and the Foreign Intelligence Surveillance Act does not cover access to records. As with bank records, the FBI is asking for legislation that provides mandatory access for counterintelligence purposes to such telecommunications records as telephone billing records. The Committee has incorporated such legislation in the Intelligence Authorization Act for Fiscal Year 1987.

A third gap in federal law concerns physical searches. The Foreign Intelligence Surveillance Act (FISA) authorizes a special court composed of Federal District Judges to grant orders for electronic surveillance to meet counterintelligence requirements, but the Act does not apply to physical search. The FBI supported broadening the Act to cover searches as part of the intelligence charter legislation considered by the Committee in 1980, but the only provisions of the charter to be enacted were the congressional oversight authorities. Pursuant to Executive Order 12333, the Attorney General authorizes warrantless searches for counterintelligence purposes.

The absence of a statutory court order procedure creates at least two problems. First, as with bank and telephone records, there is no authority to require cooperation from private parties. Second, the Federal appeals court in the *Truong* case ruled that evidence derived from a warrantless counterintelligence search may not be used in court if the search occurs after the Government decides to prosecute. Neither problem exists for wiretaps and other forms of electronic surveillance under the Foreign Intelligence Surveillance Act, which provides a court order procedure to secure the cooperation of private parties and permits the use of information for law enforcement purposes with appropriate security.

In light of this situation, the Committee recommended in 1984 that legislation be developed to establish statutory procedures comparable to FISA for physical search. The Committee is prepared to develop and introduce such legislation in cooperation with the Executive branch.

The President's interim report to the Intelligence Committees comments, "It is imperative that FISA be retained as it now exists." The Committee similarly endorsed FISA in 1984, finding that it has resulted in "enhancement of U.S. intelligence capabilities" and also "contributed directly to the protection of the constitutional rights and privacy interests of U.S. persons." The Committee believes that physical search legislation can be achieved, with Executive branch support, without endangering FISA.

Espionage investigations and prosecutions would also be more successful if greater expertise and resources were brought to bear in certain areas. Since 1985 the Army has reorganized its counterintelligence efforts and instituted a specialized training program to develop greater expertise at the field level in espionage investigations.

The espionage prosecutions in 1985 and 1986 demonstrated the importance of early consultation with Justice Department attorneys in developing tactics that reconcile intelligence and law en-

forcement interests. In the Pelton case, close cooperation between NSA, and the FBI, and the Justice Department resulted in a conviction with minimal disclosure of sensitive information. In the Sharon Scranage case, the combined efforts of the CIA, the FBI, the Justice Department, and the State Department produced a strategy that successfully led both to two convictions and to the exchange of the Ghanaian official convicted in the case for several prisoners in Ghana and their families.

The Committee understands that such consultation is now being instituted in a more timely manner than often occurred in the past. This welcome coordination requires that the Justice Department, in turn, have a sufficient number of attorneys trained and experienced in handling the unique problems in these cases. The Committee is especially concerned that those attorneys learn how to maintain controls on the release of sensitive information. Department attorneys should also work with U.S. counterintelligence agencies in potential espionage cases to ensure that their methods are as consistent as possible with successful prosecution. In this regard, the Justice Department's Criminal Division has begun to build a cadre of experienced personnel and to provide additional training to United States Attorneys.

The Howard case, which is discussed in some detail in the Committee's classified Report, revealed serious shortcomings in CIA performance relating to espionage investigations. The Committee is pleased to learn that the CIA has taken steps to correct problems pinpointed in investigations by its Inspector General and an interagency group. The Committee will monitor the implementation of those changes.

Issues relating to the handling of the Howard case by the FBI and the Justice Department have also been pinpointed and are the subject of continuing consideration. The Committee expects remedial actions to be taken, as appropriate, and will continue to follow this matter.

Findings and Recommendations

22. Recommendation.—The United States should not tolerate violation of our espionage laws by any country and should investigate the intelligence operations of countries that control or permit the commission of espionage in or against the United States on their behalf. The Committee is pleased to learn on their behalf. The Committee is pleased to learn that the State Department has pledged to cooperate with enforcement action whenever evidence of espionage is presented, and the Committee supports efforts to set up a mechanism for regulatory interagency consultation on cases that might warrant action.

23. Finding.—The Foreign Intelligence Surveillance Act continues to be considered by U.S. counterintelligence agencies to be highly beneficial to their efforts. They strongly favor retention of FISA as it now exists.

24. Recommendation.—Congress should enact legislation to give the FBI the authority to require financial institutions and telecommunications carriers to provide access to records, with notice restrictions comparable to FISA. Any such authority should be limited to counterintelligence matters, governed by the current Attor-

ney General's guidelines, and accompanied by improved provisions for congressional oversight.

25. Recommendation.—Congress should enact legislation comparable to FISA to authorize physical search for intelligence purposes, so as to reduce legal uncertainties in counterintelligence investigations that have prosecution as one of their objectives.

26. Recommendation.—U.S. counterintelligence agencies should continue to emphasize, as standard procedure, consultation with the Justice Department at an early stage in potential espionage cases. The Justice Department should provide increased training to Criminal Division attorneys and U.S. Attorneys concerning the prosecution of espionage cases, including the need to protect sensitive information relating to such cases.

27. Finding.—The CIA has taken some steps that are likely to improve counterintelligence investigations and prosecutions, in the wake of investigations of the Howard case. The Committee will monitor implementaton of those improvements.

28. Recommendation.—The FBI and the Justice Department should take actions, as appropriate, to remedy shortcomings exposed by the Howard case.

E. OVERSEAS OPERATIONS

Strategic counterintelligence objectives abroad differ from those in the United States not only because of the different environment, but also because of the added requirements for counterintelligence support in intelligence collection programs. The Committee welcomes recent CIA initiatives to improve both its counterintelligence efforts and its career opportunities in counterintelligence.

The Committee's classified Report discusses further issues regarding CIA and Department of Defense counterintelligence activities overseas.

The investigation of espionage by U.S. civilian and contractor personnel abroad raises jurisdictional questions. The Committee believes that the FBI should be called in and should work closely with agency security officials from the outset.

Findings and Recommendations

29. Finding.—The CIA has begun initiatives to improve its counterintelligence efforts.

30. Recommendation.—U.S. agencies abroad should continue to obtain the timely advice and assistance of the FBI in cases of possible espionage by civilian and contractor personnel.

F. PERSONNEL MANAGEMENT AND TRAINING

Counterintelligence is not the main function of any of the organizations responsible for U.S. counterintelligence programs. The CIA's primary task is collection and analysis of political, economic and military intelligence; the FBI is a law enforcement organization; and each of the service counterintelligence organizations is part of a larger criminal investigative or intelligence agency. This is one reason why there have been less specialized training and fewer incentives for careers in counterintelligence. Personnel are recruited for law enforcement or intelligence positions generally

and are usually not assigned to counterintelligence until they have experience in other fields. The advantage of this practice is that personnel can develop their basic investigative or intelligence skills in less sensitive areas before taking on more important counterintelligence duties. The disadvantage is that specialization and career advancement in counterintelligence may be discouraged because of the organization's emphasis on other functions.

Every agency is taking steps to upgrade counterintelligence training, but the results thus far have been uneven. More should be done to encourage agencies to share their experience with successful methods. While each agency operates in a different environment and with different internal regulations, joint discussion of such topics as the nature of the threat from particular hostile services and the techniques for offensive operations and counter-espionage investigations could be very useful. This would also make more efficient use of expert personnel who assist in other agencies' training. In the CIA and the military services, better training in agency guidelines is also needed.

In the aftermath of the Miller case, the Committee has taken a close look at FBI personnel management policies for counterintelligence. At the Committee's request, the FBI prepared a study reviewing the impact of FBI personnel policies on the Foreign Counterintelligence (FCI) Program in order to determine how the FBI may more effectively recruit, select, assign, train, promote, and retain Special Agents for counterintelligence matters. The FBI study indicated a need for improvements in several areas.

The FBI confronts unusual personnel management problems because of the large hostile intelligence presence in New York City, where the cost of living has discouraged FBI Agents from seeking assignments or pursuing careers. Unlike State Department personnel, FBI Agents in New York do not have a special housing allowance to defray the cost of living in town. The Committee believes that action is needed to improve benefits and incentives in New York and is prepared to develop legislation that may be needed for this purpose.

Another manpower issue is the limited number of FBI senior grade positions in the counterintelligence field, as compared to positions as Special Agent in Charge of a field office and comparable headquarters positions with primarily law enforcement duties. The Committee supports efforts to change this situation, including funds requested in the FY 1987 budget to increase the number of senior grade counterintelligence positions at FBI Headquarters. The Committee also supports the FBI policy requiring that all new Special Agents in Charge of field officers who have not previously served in a full-time counterintelligence position must receive FCI training.

The Committee intends to continue its review of FBI counterintelligence personnel policies as part of a broader ongoing study of intelligence community personnel issues.

DoD counterintelligence components have similar problems and should develop appropriate revisions in personnel policy to encourage specialized counterintelligence career development. In all the DoD counterintelligence units, as well as the FBI, greater efforts are needed to recruit and retain the best possible personnel.

Findings and Recommendations

31. Recommendation.—More should be done to encourage agencies to share their experience with successful CI methods and to make more efficient use of expert training personnel.

32. Recommendation.—Additional measures should be taken to improve benefits and incentives for FBI Agents in New York City, including any legislation needed to give the FBI comparable authority to the State Department.

33. Finding.—The FBI is planning to increase the number of senior grade counterintelligence positions at FBI Headquarters. The Committee supports these efforts.

34. Recommendation.—While each counterintelligence agency must recruit to satisfy its unique needs, greater attention should be given to determining specialized qualifications required for personnel to meet each agency's CI needs as distinct from law enforcement or foreign intelligence needs.

35. Recommendation.—DoD counterintelligence components should continue to develop appropriate revisions in personnel policy to encourage specialized counterintelligence career development.

IV. Security Countermeasures

In 1984-85 the Executive branch conducted seven in-depth studies of security policies and practices for protecting classified information and activities against hostile intelligence collection. The Committee has reviewed findings and recommendations from all of these studies, as well as observations and proposals made by other Congressional committees, by witnesses at the Committee's closed hearings, and by experts inside and outside the Government. Taken together, these reports and recommendations raise grave questions regarding U.S. security programs to protect sensitive information from our adversaries.

The Walker case disaster and the bugging of typewriters in our Moscow embassy were compromises that waited years to be uncovered and that illuminated significant weaknesses in the nation's security. There have been wide disparities in policies and standards for personnel, information, technical and other security measures. Serious imbalances in resource allocation have existed, and in some areas inadequate resources have led to serious gaps in protection. Research and development to improve security has been haphazard at best.

Since the late 1970s, the Committee has worked with the Executive branch and the intelligence community to strengthen counterintelligence throughout the Government, so that the FBI, CIA and DoD counterintelligence components could deal more effectively with the hostile intelligence threat. Until 1985, however, neither this Committee nor any other congressional body had taken a similarly comprehensive look at the defensive security countermeasures that surround the core of classified information and that are supported by counterintelligence. The Committee's closed hearings in the fall of 1985 were the first systematic Congressional review of security programs since the 1957 report of the Commission on Government Security established by Congress (with Senator John Sten-

nis as its Vice Chairman). Although the Committee is encouraged by many of the steps now being taken to remedy serious deficiencies, the continuing fragmentation of security planning and policy requires a substantial reorganization of the way the Government handles its many security programs. Congress has a similar duty to put its own house in order; and the Committee has specific recommendations for that purpose as well.

The Committee has addressed security countermeasures at two levels. First is the national policy level, where government-wide initiatives and programs are developed, approved and overseen. Many of the most serious security weaknesses result from the lack of an effective, national policy that gives high priority to security programs and ensures comprehensive and balanced planning. The second level is the numerous separate security disciplines, which each have their own problems that must be solved within a coherent national policy framework. These disciplines include information security, personnel security, communications security, computer security, emanations security (TEMPEST), technical surveillance countermeasures, physical security, industrial security and operations security. Their variety itself clearly indicates how difficult it is to pull together the necessary expertise and reconcile the interests of different agencies and programs—intelligence, military, diplomatic, industrial, research and budgetary. Nevertheless, the effort must be made if we are to reduce the likelihood of future compromises that repeat the multi-billion dollar damage of the Walker, Pelton, Howard, Harper and Bell cases or the incalculable harm from interception of our communicatins and technical penetration of U.S. facilities.

We would not wish to mislead; in any foreseeable environment, U.S. security countermeasures programs can provide no absolute guarantees against compromises and losses. Our goal is a significant improvement in security, a further limiting of the damage that is wreaked by those compromises and losses. Our belief is that more effective, but not unduly intrusive measures can accomplish this objective.

A. A NATIONAL STRATEGIC SECURITY PROGRAM

In December, 1985, the Committee recommended to the National Security Council that the Excutive branch develop a comprehensive and integrated National Strategic Security Program to coordinate and foster the protection of sensitive information and activities from the efforts of hostile intelligence services. The purpose is three-fold.

First, such a program would give greater visibility, higher priority and increased attention of senior officials to security countermesures. Frequently, security programs have neither an influential voice in government departments and agencies nor adequate funding and career opportunities. Security must be recognized by the Executive branch and Congress as a crucial underpinning to the other basic functions—military, intelligence and diplomatic—that safeguard national security.

Second, the reason for such a program is to provide a coherent structure to address and overcome security deficiencies. As dis-

cussed in the following sections, these problems include underfunding of essential programs, significant gaps in research, inadequate training and career development, insufficient management accountability, uneven national policy guidance, interagency conflicts over new initiatives, and failure to ensure necessary linkages among security disciplines.

Third, the establishment of such a program and structure should provide long-term continuity and consistency through succeeding Administrations. The changing of NSC structures from one Administration to the next does not fill the pressing need for continuity and consistency of policy. When a National Strategic Security Program has taken shape, therefore, the essential features should be promulgated by the President in a formal Executive Order.

At the Committee's closed hearings in late 1985, senior officials were asked to discuss how U.S. counterintelligence and security countermeasures policies are established and coordinated at the national level. The answer for counterintelligence was clear: responsibility is focused on a single NSC committee process (the Interagency Group for Counterintelligence (IG–CI) and the Senior Interdepartmental Group for Intelligence (SIG–I)), with support from an interagency staff which assists the NSC staff in coordinating policy initiatives and overseeing their implementation. Much progress has been made in developing a coherent process for counterintelligence policy. The same cannot be said for security countermeasures, where responsibilities have been widely diffused and the Executive branch has only begun to develop a coherent policy review structure.

The DCI testsified that the SIG–I is "the principal forum where the national perspective can be brought to CI [counterintelligence] and CM [countermeasures] policy," with countermeasures handled by an Interagency Group (IG–CM) chaired by the Deputy Undersecretary of Defense for Policy. At the same time, however, the DCI acknowledged the existence of "other Executive branch policy recommending and implementing entities such as the DCI Security Committee, the National Telecommunications and Information Systems Security Committee, the SIG for Technology Transfer, etc." While the DCI said the SIG–I system has " the capability for and mission for ensuring proper national-level coordination of all CI and CM matters," this has not in fact been the case for security countermeasures.

Recently, the DCI, acting in his capacity as Chairman of the SIG–I divided the Interagency Group for Countermeasures into separate groups for Technical matters (IG–CM(T)) and for Policy and other non-technical issues (IG–CM(P)). The new IG–CM(T), headed by the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, is intended in part to serve as a bridge between the intelligence world of the SIG–I and the world of the National Telecommunications and Information Systems Security Committee (NTISSC). The NTISSC is chaired by the same Assistant Secretary and has a presidential mandate under NSDD–145 to develop communications, computer and emanations security policy for the whole government.

The DCI also abolished the DCI's Security Committee (SECOM), which had been a working-level intelligence community group out-

side the IG–CM but covering some of the same issues. The two new IG–CMs are to have subcommittees that will handle many of the former SECOM functions, but with more senior members than was the case with SECOM, so that subcommittee members can actually commit their agencies to act upon group recommendations. Staffing is to be achieved through an up-graded interagency staff.

These structural changes are very welcome signs of the seriousness with which the Executive branch is approaching the need to improve the security policy process. The Committee does not believe, however, that they go far enough in establishing a forum in which all the many security interests can be surfaced and reconciled. It is uncertain, moreover, whether the IG–CM subcommittee will be sufficient improvements on the SECOM structure to overcome the bottlenecks that too often have stifled progress on security issues. The Committee continues to believe, therefore, that a comprehensive National Strategic Security Program must be developed, through whatever structures the Executive branch finds best suited to that task.

In recommending establishment of a comprehensive National Strategic Security Program, a Committee does not intend to create a "czar" or to take from individual agencies their responsibility for implementing national policies that affect their work. If there is no national policy, however, there is no standard against which to hold each department accountable. If national policies are fragmented, outdated or unbalanced, security becomes subordinated to other departmental priorities and interagency disputes. This has occured far too often in recent years. Later sections of this Report give examples: the inability to reach agreement on a "single scope" background investigation for Top Secret and SCI clearances; the proliferation of special access programs without sufficient controls and standards; the imbalance in resources between expensive technical safeguards and the personnel and information security measures needed for effective computer security; and, at least until very recently, interagency conflicts over how to deal with some technical security issues.

As important as it is to remedy these problems, the greatest value of a National Strategic Security Program should be to promote innovative solutions to new and emerging hostile intelligence threats. This requires collaboration with counterintelligence agencies to identify such threats, as well as recruitment and training of top-quality security specialists with wide-ranging operational, technical, analytical, and managerial skills. At the core must be a commitment at top management levels within each department and agency to setting clear security objectives, providing adequate resources, and devising effective oversight and inspection procedures for holding managers and commanders accountable for their performance. This commitment will be forthcoming only if Congress and the President make clear they expect it and establish their own systematic means to assess government-wide progress in meeting national goals.

A National Strategic Security Program should provide policy direction and oversee implementation for all security disciplines:

Personnel security;
Information security;

64-268 O - 86 - 3

Communications, computer and emanations security;
Technical surveillance countermeasures;
Physical security;
Industrial security;
Operations security.

To assist the NSC, a single body shoud be assinged responsibility for policy planning and analysis of all aspects of security countermeasures for protection of sensitive information against hostile intelligence efforts. It should ensure effective coordination among the other interagency forums that address particular problems. It should have the task of putting together for the NSC and the Congress a fully balanced and coordinated government-wide program. A senior official should be designated to testify on the National Strategic Security Program before the appropriate Congressional committees.

During 1985, the CIA and the State Department took significant steps to achieve the same objectives on a departmental level. The CIA reorganized and expanded its Office of Security to integrate all its security functions. Similarly, as recommended by the Inman Panel on Overseas Security, the State Department established a new Diplomatic Security Service with higher status and wider responsibilities, including a high-priority effort to upgrade technical security. The Stilwell Commission has recommended a similar action by the Defense Department, stressing "that all security disciplines have as their fundamental purpose the protection of classified information and must be applied in a fully balanced and coordinated way." The Committee urges that resources be allocated to enhance security policy and oversight in the Office of the Secretary of Defense (OSD), so as to make the policy-level integration of the various security programs in DoD a viable option.

A significant aspect of the National Strategic Security Program should be to assist the NSC on resource priorities. The current budgetary arrangements are fragmented and inadequate. To consider ways to improve the resource allocation process, the Committee held a closed hearing on June 4, 1986, on principal security programs outside the NFIP, as well as those in the CIA Office of Security. The ultimate goal of the Committee is to have each department and agency identify its security resources by function and program and include these resources in their congressional budget justification submissions. The National Strategic Security Program should give the NSC and Office of Management and Budget a similar opportunity to evaluate the resource priorities of these and other security countermeasures programs.

Another high priority for the National Strategic Security Program should be an assessment of requirements for research and analysis, especially on personnel security and the interfaces between personnel, communications and computer security. The greatest imbalance in security resources is between costly projects on technical safeguards and the meager efforts to look into personnel security issues. Not until January, 1986, was DoD able to get the necessary concurrences for a modest personnel security research program in DoD to be administered by the Navy. Current arrangements for intergency assessment of security research needs have been insufficient to identify and promote aggressive and bal-

anced government-wide efforts, even though particular agencies have taken valuable initiatives in areas of concern to themselves.

Special emphasis should also be placed on commander and manager responsiblity for security within their respective organizations. The recent action of the Deputy Secretary of Defense ordering the incorporation of security management as a criterion in military and civilian performance and fitness reports is a step in right direction. Such a requirement should be extended government-wide and apply to all contractors as a condition for inclusion on a bidders list. Other realistic sanctions are needed, as well as greater consistency in the government and among contractors on the severity and application of such sanctions as fines, relief for cause, debarment and suspension, for knowing or negligent security violations both by managers and by subordinates. The National Strategic Security Program should supply the necessary policy direction.

Security normally ranks well below other careers in most agencies; the National Strategic Security Program must change the status of the security profession. Security specialists should match other professionals in terms of their qualifications, training, compensation and career opportunities. There should be an independent evaluation of the recruitment, training, pay, status, professional development and retention of federal security officers in all departments and agencies. As recommended by the Information Security Oversight Office and the Stilwell Commission, the OPM job classification standards for security should be revised immediately to ensure comprehensive and accurately graded descriptions of modern security disciplines.

One of the common themes in all recent studies of security countermeasures—the Information Security Oversight Office (ISOO) task force, the Stilwell Commission, and the Inman Panel—is the need for better training not only for security professionals, but also for managers and other officials having security responsibilities. In the near-term, the quality of training for new security personnel must have special attention. Through the government, security initiatives are providing funds for new personnel. Agencies should be held accountable for ensuring that the most qualified personnel are recruited and that their training meets high standards.

The National Strategic Security Program should establish government-wide security training objectives for managers, security professionals, personnel security clearance adjudicators, and industrial security officiers. Minimum levels of training and certification should be established for industrial security personnel, clearance adjudicators, and other positions requiring consistent standards. Because the Defense Investigative Service and the Defense Security Institute (DSI) have crucial roles in the development and implementation of security training programs and industrial security generally, an expanded government-wide training role for DSI should be considered. The Information Security Oversight Office has made a similar recommendation. DSI could serve as a national security training and education center serving all federal departments and agencies. Consideration should also be given to forming under DSI an interagency group, with counterintelligence agency participation, to develop and review effective security awareness

educational material and techniques. Given the concentration of sensitive facilities on the West Coast, establishment of a permanent West Coast security training facility for government and contractor personnel should be considered.

One of the most challenging and difficult tasks that a National Strategic Security Program must address is the development of coherent and effective policy for operations security (OPSEC). OPSEC has many definitions amoung the various departments and agencies. It can include the implementation and assessment of U.S. efforts to frustrate hostile intelligence collection. Another element is the careful design of particular unclassified activities or information to keep hostile intelligence services from putting together bits and pieces of information to detect classified missions or the presence of sensitive installations.

Equally important is the assessment of government practices outside the national security field that could help or hinder hostile intelligence collection efforts. The recently established National Operations Security Advisory Committee of the IG-CM(P) has taken several valuable initiatives in restricting public availability of sensitive data.

A 1985 interagency assessment identified serious OPSEC weaknesses. The National Strategic Security Program should develop government-wide OPSEC objectives and ensure that relevant agencies have the necessary resources and programs to achieve these goals. Just as sensitive military units take care to ensure that changes in routine activity will not provide our enemies indications and warning of their operations, so must agencies and contractors involved with sensitive agencies or programs incorporate OPSEC in their overall security philosophy and programs.

These are some of the government-wide security issues that should be addressed by a National Strategic Security Program. Others are detailed in the sections below on personnel security; information security; communications, computer and emanations security; technical and physical security; and industrial security.

Findings and Recommendations

36. Recommendation.—The Executive branch should develop and implement a comprehensive National Strategic Security Program which would provide:

a. NSC-approved objectives and policy direction;

b. A broad master plan faithful to the objectives and policies, and both based upon and prioritized in light of the threat;

c. Close coordination of implementing programs;

d. Assessment and allocation of resource requirements for all areas of common concern—such as, but not limited to: R&D; computer security; TEMPEST and personnel security; and core training for technical security countermeasures;

e. Oversight of implementation of national policy; and

f. A review of total resources planning.

This program, although within the NSC, should be structured so as to provide long-term continuity and consistency through succeeding Administrations. Accordingly the program and the essential structure for its maintenance should be promulgated by the President in an Executive Order.

37. Finding.—Recent IG-CM changes promulgated by the DCI, although not sufficient, in the Committee's view, to solve the problem, are a welcome sign of the seriousness with which officials are addressing the need to improve the security process.

38. Recommendation.—The Defense Department should enhance its security policy and oversight capabilities in the Office of the Secretary of Defense so as to ensure integration of policies for the various DoD security programs

39. Recommendation.—The National Strategic Security Program should evaluate security countermeasures resource priorities for the NSC and OMB on an annual basis. Security resources should be identified by function and program in departmental and agency budget justifications. The Administration and the Congress should consider additional ways to implement a more coherent budget process for security programs.

40. Recommendation.—The National Strategic Security Program should assess requirements for research and analysis on security countermeasures to promote aggressive and balanced efforts government-wide, especially on personnel security.

41. Recommendation.—The National Strategic Security Program should emphasize commander and manager responsibility for security, including government-wide application of the recent DoD action to incorporate security into performance evaluations and development of more realistic and consistent policies for disciplinary sanctions.

42. Recommendation.—The National Strategic Security Program should commission an independent evaluation of the recruitment, training, pay, status, professional development and retention of federal security personnel. Relevant OPM job classifications should be revised and modernized.

43. Recommendation.—The National Strategic Security Program should establish government-wide security training objectives and should require minimum levels of training and certification for industrial security officers, clearance adjudicators, and other positions requiring consistent standards.

44. Recommendation.—The National Strategic Security Program should consider phased assignment of national responsibilities for security training to the Defense Security Institute (DSI), with an interagency group including representation from U.S. counterintelligence agencies to develop security awareness materials. DSI should establish a West Coast annex.

45. Recommendation.—The National Strategic Security Program should develop government-wide operations security (OPSEC) objectives and ensure that relevant agencies have the necessary resources and programs to achieve those goals.

B. PERSONNEL SECURITY

The most important barrier to the hostile intelligence threat and the growing willingness of Americans to divulge classified information for financial gain is a sound personnel security program. Unfortunately, recent Executive branch and congressional studies have identified significant weaknesses in U.S. Government personnel security practices. Many of the issues raised by the Report of

the Commission on Government Security in 1957 remain unresolved today, particularly the need for national policy guidance and oversight. The Stilwell Commission, the DoD Industrial Security Review Committee (formed after the Harper espionage case), the Permanent Subcommittee on Investigations of the Senate Governmental Affairs Committee, other interagency assessments, and investigations of agency performance prompted by recent espionage cases have all addressed deficiencies, inconsistencies and ineffectiveness in the administration of personnel security policies and programs. Development of a more coherent and effective personnel security policy should have the highest priority in a National Strategic Security Program.

The Stilwell Commission, while finding the DoD security program "reasonably effective," made the following critique:

> Clearly there is room for improvement. Many people are cleared who do not need access to classified information. Background investigations yield relatively little derogatory information on those being cleared, and under the existing adjudication process, far fewer still are actually denied a clearance. Once cleared, very little reevaluation or reinvestigation actually occurs, and relatively few indications of security problems are surfaced. The principle that a cleared individual is authorized access only to that information he "needs to know" is generally not enforced.

The Commission attributed these problems to insufficient resources and the desire not to let security interfere with mission accomplishment.

The Committee endorses vigorous implementation of most of the Stilwell Commission's recommendations on gaining and maintaining access to classified information and on detecting and investigating security violations. They should be reviewed at the NSC level and adopted for government-wide application. In summary, the Commission proposes:

For Secret clearances, better background checks, an eventual reinvestigation system, and better workplace controls (document logs and briefcase searches).

For Top Secret information, many more reinvestigations, more polygraphs primarily for reinvestigations, better workplace controls (a personal reliability program and a ban on one-man access), and a special crypto-access compartment.

More inspections and management responsibility.

Not issuing clearances for information to personnel who require only access to the workplace.

Measures to reduce the number of clearances and streamline security requirements for contractors, including a billet system to cut the number of Top Secret clearances, justification for each contractor clearance (with periodic rejustification for overseas positions), and a single scope for Top Secret and SCI background investigations.

To free resources to cover other costs, the easing of reinstatement procedures for contractors whose clearances lapse for a short time and the routine granting of interim Secret clearances while initial investigations are conducted.

These recommendations reflect the most comprehensive and detailed analysis of DoD personnel security requirements that has been conducted in decades. Nevertheless, in some respects they fall short of meeting current needs.

The first requirement is resources. Personnel security is seriously underfunded, especially in comparison to the technical programs for communications and computer hardware and software. Redressing this imbalance should be one of the highest priorities for a National Strategic Security Program. Congress added $25 million for the Defense Department in FY 1986 to reduce the backlog of investigations and, especially, of reinvestigations of persons with Top Secret clearances. The Committee has recommended, and the Senate has passed, an additional $22 million authorization and 358 positions for FY 1987 to accelerate implementation of Stilwell Commission recommendations, primarily regarding more detailed investigations for Secret clearances. Intelligence elements have also regularly fallen short of meeting periodic reinvestigation goals because of inadequate funding. This is true as well for the FY 1987 budget. The basic problem is that personnel security has had relatively low priority in the Executive branch budget process. The Committee welcomes recent testimony by the DDCI that the CIA will give much higher priority to reinvestigations.

Nowhere is the adage "penny wise, pound foolish" more apt, yet even the Stilwell Commission had to confront serious resource constraints. Its goal is to reduce the DoD backlog of reinvestigations for persons holding Top Secret clearances to manageable levels within four years and to conduct periodic reinvestigations of all persons holding Secret clearances and above by 1995. Efforts to reduce the number of positions requiring background investigations can alleviate some of the pressure, but the technological sophistication of modern military systems and the need for widespread access to intelligence products requires that large numbers of DoD personnel have at least Secret-level clearances. On the civilian side, the work of Departments such as State, Energy, Justice and Treasury will continue to require that many employees have background investigations and reinvestigations.

Over the years, resource constraints have prevented any serious consideration of field investigations for Secret clearances, which have been based on name and fingerprint checks of law enforcement and counterintelligence files. Some of the most sensitive information in the U.S. Government is classified at the Secret level, and sustained passage of Secret information to hostile countries would do grave damage to national security in many areas. The Harper case is a good example where compromise of a substantial amount of Secret information from a defense contractor's office did great harm. The current requirements for Secret clearance investigations are too low, and the proposals for wider checks are too modest.

At a minimum, the investigative requirements for a Secret clearance should include, in addition to file checks: a credit check; inquires to present and past employers; more documentation of identity; other field inquiries on recent life history; and a subject interview. The key is the interview, to surface issues that may merit further investigation. This recommendation requires a substantial

increase in manpower and funds, but the cost is reasonable in light of the Soviet bloc intelligence emphasis on acquisition of Secret-level technological data.

Overall, the Stilwell Commission goal of eliminating the reinvestigation backlog within four years should be extended government-wide and to contractor employees. In addition, a government-wide plan for Secret clearances should be developed and submitted to the Committee, with a target of implementation in less than the ten years proposed by the Stilwell Commission. A government-wide funding plan to achieve all these objectives should be submitted to Congress as soon as possible.

Another resource problem results from the resistance of some authorities to modification of Top Secret and SCI background investigation requirements that Defense Department officials have concluded are not cost-effective. Because the Defense Investigative Service, CIA and OPM have different policies on the scope of those investigations, it is not unusual for individuals, particularly in industry, to have two or more background investigations in the same year for Top Secret and SCI access. Moreover, some agencies appear unwilling to simplify their background investigation procedures in the light of cost-effectiveness studies. While the Committee has not attempted to evaluate alternative procedures in detail, it strongly recommends that a uniform policy be established to achieve less costly and more timely background investigations and clearances and to eliminate redundant investigations.

Another factor that should guide development of a "single scope" investigation is the high priority for reinvestigations. Recent espionage investigations indicate that none of the current approaches to initial clearance is infallible. Espionage-related issues rarely surface during initial background checks. Streamlining the procedures for initial investigations would release manpower for use in meeting the five-year reinvestigation requirement that all agencies agree should apply to Top Secret and SCI Clearances.

The Committee also believes that a "single scope" background investigation for Top Secret and SCI clearance should include an in-depth interview of each subject by a trained and experienced security officer. The record indicates that such interviews are often effective in surfacing issues not uncovered by a field investigation that bear on the ability of an individual to handle sensitive information.

Several Stilwell Commission proposals deserve special emphasis. A reliability clearance for persons needing access to a site, but not to classified information, would underscore the importance of "need to know." There are no figures on the number of people with clearances where the intent is solely to determine their reliability. Included in this category are guards, char force, maintenance personnel, etc. Implementation of this measure would set the stage for carrying out such other measures as a "billet control system" describing which positions require access to classified information. This action will help revive the need-to-know rule by drawing a clear distinction between clearance for one purpose and clearance for other purposes.

The Committee shares a concern, expressed initially by the Permanent Subcommittee on Investigations, about the potentially seri-

ous risks in issuing security clearances to foreign-born individuals whose background cannot be verified adequately. The Stilwell Commission's proposal for use of the polygraph in such cases is comparable to the FBI's policy of polygraphing foreign nationals employed for specialized purposes. Agencies must guard against overreliance on the polygraph, of course, especially when independent corroboration is so difficult to obtain. Other approaches tailored to particular agency needs should also be considered. A government-wide minimum standard is needed, however, in order to ensure cross-agency acceptance of clearances.

One Stilwell Commission recommendation that should be reconsidered is the proposal for one-time, short duration (read on, read off) access by cleared personnel to the next higher level of classified information when necessary to meet operational or contractual exigencies. Given the vast differences between investigative standards for Secret and Top Secret, there is too great a risk in giving an individual with only a Secret clearance access to Top Secret information. If the requirements for Secret clearances are substantially upgraded, this proposal could be reconsidered as a means to conserve security resources. As the Stilwell Commission recognized, administrative oversight is essential to ensure that repeated read on, read off access does not become a loophole for semipermanent access.

Several areas of concern not mentioned by the Stilwell Commission deserves serious consideration. One is the need for relevant data on persons who leave positions with Top Secret or sensitive compartmented accesses. Pelton, Howard and, for the most part, Walker committed espionage after each had lost his clearances.

Walker's greed and his aberrant conduct as a private investigator could have alerted a Navy system tasked to continue oversight of individuals with previous high clearances. No such system effectively exists. Pelton's bankruptcy should have served as the indicator for further NSA review, particularly in view of Pelton's access to very sensitive information. Had Howard's travels and finances been known, the FBI might have been brought into that case much sooner.

The Executive branch should consider requiring as a precondition for clearance, that those who receive access to the most sensitive information agree to permit, for a period of years after their clearance ends, access to relevant financial and foreign travel records. In practice, for example, this would mean that agency security officials could access credit bureau information on former employees, as DoD agencies are now doing on background investigations and reinvestigations pursuant to the Stilwell Commission's recommendation.

Such a system could be abused if not clearly limited to persons with access to especially sensitive information and properly administered under stringent safeguards for privacy and civil liberties. It would be important to establish clearly, for example, that the examination of these records would not imply suspicion regarding a person. Another useful safeguard might be to limit the information gained from these records to an employee's security file unless the Director of Security certified that it warranted the attention of another office or the FBI. Other minimization procedures, perhaps based upon those in the Foreign Intelligence Surveillance Act,

could also be applied. In addition to providing better means to detect suspicious behavior, records access procedures could enable security offices to respond in a timely and helpful fashion to evidence of financial problems among personnel whose recent sensitive accesses would make them lucrative intelligence targets.

The Committee recommends that the Executive branch study the possibility, in consultation with appropriate congressional committee and civil liberties experts, of a program of expanded post-access foreign travel reporting obligations and/or agency access to relevant financial and travel records. The Committee believes that such a program, if combined with proper safeguards and limited to those persons whose access to the most sensitive information clearly warrants special measures, might be acceptable from a civil liberties standpoint. A similar view has been expressed by a ranking ACLU official at a recent conference sponsored by the Congressional Research Service of the Library of Congress.

Another initiative, relevant to the role of a National Strategic Security Program in fostering and coordinating research, is examination of the value of psychological testing in the security clearance process. Some authorities contend that such testing can help identify persons disposed to disregard their obligations for the sake of self-gratification. Any use of psychological testing, however, should take full account of the need for test reliability, trained personnel to interpret results, and protection of individual rights. Psychological testing can supplement, but not replace other screening devices.

The Stilwell Commission urged the Secretary of Defense, although not in a formal recommendation, to press for revival of the interagency effort chaired by the Justice Department in 1983–84 to draft a new Executive Order on personnel security. While drafting such an order may be a lengthy process and must not be an excuse for inaction on the specific national policy issues discussed above, a new Executive Order would make an important contribution to better personnel security. Such an order should provide a formal Presidential mandate for minimum government-wide standards and procedures that incorporate the essential elements of national policy on key topics, with details to be spelled out in an implementing directive that can be updated periodically in light of experience and research. Second, it should establish an office similar to the Information Security Oversight Office to provide the kind of policy guidance and oversight of implementation that ISOO has supplied for information security. The absence of such an office makes it extremely difficult for the National Security Council to address personnel security policy issues government-wide. Third, a new Executive Order should focus exclusively on policies and procedures for access to classified information and to facilities where classified information is maintained. Experienced Justice Department officials believe that such an order would make it easier to defend in court decisions to deny or remove security clearances.

More extensive and timely background investigations and reinvestigations, with streamlined government-wide standards and procedures, must feed into an adjudication system with rigorous but realistic criteria for granting or denying clearances. There is currently no uniform requirement to deny a clearance to a person who

has been convicted of a felony or has admitted to conduct which constitutes a felony under state or local law. There is no requirement for follow-up inquiries in cases where clearances are granted to persons admitting problems like drug use. (The FBI has expressed particular concern about this problem in contractor facilities, where habitual drug users have posed real threats to sensitive research and development programs.) There is no government-wide requirement for training of persons who adjudicate security clearance cases. (Only one agency currently has a formal adjudicator training school and individual services tend to have too few adjudicators to justify their own training programs.) The lack of training and experience among adjudicators causes delays and inconsistencies within and among agencies.

Agency and interagency investigations of such recent espionage cases as Edward Lee Howard and Jonathan Pollard have highlighted serious flaws in agency hiring, assignment and termination practices. The CIA and DoD have moved to rectify problems, and there will probably be interagency consideration of adopting similar corrective measures. The CIA and other agencies have also become more sensitized to the risks inherent in decisions to give sensitive assignments to persons with a history of personal problems. While there is a balancing need not to do away with necessary managerial flexibility, these corrective steps are basically much needed and long overdue.

Underlying these specific problems is a general attitude that the purpose of the clearance process is simply to wed out those individuals most obviously likely to pose a threat to security. Wider background checks will have little impact if the results are not used effectively. Especially for Top Secret clearances and for the most sensitive Secret clearances, the policy should be reversed. Clearances should go to individuals whose records demonstrate a clear aptitude for security. That is, their background and personal qualities should show a high sense of responsibility—not just the absence of proved disqualifying factors. At the same time, denial of such highly sensitive clearances should not affect the ability to pursue careers in other areas.

A final personnel security issue is the use of polygraph examinations as part of the initial clearance process or in reinvestigations. Since 1983, the Committee has followed closely the various attempts in the Executive branch to widen use of polygraphing for personnel security purposes and congressional efforts to control such practices by statute. The Committee has consistently supported the approach taken by the Senate Armed Services Committee in approving a personnel screening polygraph test program for the Defense Department. That test program is limited to counterintelligence-related questions and has very stringent quality controls and safeguards for individual rights. The same limitation, controls and safeguards should apply to any expansion of polygraphing in other departments and agencies. The National Strategic Security Program should ensure full coordination of departmental policies and practices for this purpose.

The Committee is concerned about the tendency to place an overreliance on the polygraph, thereby allowing apparent passage of an examination to validate the reliability of an individual who may be

intent on espionage. Other concerns are the persistent underfunding for implementation of some high-quality polygraph programs and the risks that incompetent or improper use of the polygraph may harm the careers, reputations or well-being of loyal Americans. Adequate research on personnel screening polygraph practices is also lacking.

An essential prerequisite for any wider polygraph program in DoD or other agencies is a significant upgrading of the national polygraph training school managed by the Army. This training program should be the focal point for development of a government-wide approach to personnel security polygraph examinations, including equipment requirements, question format, quality controls, and use of individuals as training subjects. A model that should be studied is the Air Force Seven Screens program, which is described in a recent report to the Senate Armed Services Committee. This is a screening program that uses only counterintelligence-related questions and is designed to establish and maintain strict quality controls and respect for individual rights. The establishment of an Oversight and Review Committee and the conduct of regular inspections are especially valuable features of Seven Screens that should be considered for use in other polygraph programs. The Committee is pleased that other sensitive DoD programs are adopting the Seven Screens approach.

The Stilwell Commission recommended that Congress replace the current statutory authority for a limited DoD "test program" with permanent legislation authorizing the use of polygraph examinations for personnel screening with counterintelligence-related questions for DoD personnel. Any such legislation should incorporate standards for quality control and respect for individual rights and should provide a means whereby those standards can be enforced. DoD has prepared draft legislation for this purpose. The legislation deserves serious consideration in the next Congress, after thorough review of the current test program. If Congress does not yet have sufficient test data to decide this issue, then the current test program should be extended for a specific period, at the end of which a decision on permanent authority will be made.

The DoD-proposed polygraph legislation would apply only to the most sensitive positions and would include both quality control and oversight requirements. The Secretary of Defense and the Armed Services Committees would agree in advance to an annual numerical ceiling on examinations to be given, and no adverse action could be taken soley on the basis of polygraph results except with approval at the highest levels in special circumstances. In reviewing this proposed legislation, Congress should consider the adequacy of DoD policy oversight and inspection arrangements to ensure consistent implementation and quality control for all DoD compenents. As recommended elsewhere, this requires augmentation of OSD security policy staff personnel. An oversight and review committee comparable to SEVEN SCREENS should also be considered.

The difficulties with expanding the use of polygraph examinations in DoD and other departments suggest a need for caution at the national policy level. There is widespread misunderstanding about the use of polygraphs for personnel security screening with CI-related questions and strict quality controls. While a uniform

national policy for access to certain types of highly sensitive data is desirable in theory, more needs to be done to explain the procedures and safeguards to federal employees, the Congress and the public and to compile data on employee reactions to such examinations before a government-wide policy is implemented.

Findings and Recommendations

46. Finding.—Defense Department adoption of Stilwell Commission recommendations is a major step forward. The Committee has supported additional funding in FY 1986 and 1987 to accelerate implementation of recommendations regarding clearance investigations.

47. Recommendation.—The National Strategic Security Program should ensure substantially increased funding for personnel security in all relevant departments and agencies. A Government-wide plan should be submitted to Congress to achieve the following goals: (a) elimination of the reinvestigation backlog for Top Secret (including SCI) within four years; and (b) implementation within less than ten years of a program for intensified investigation and reinvestigation for Secret clearances.

48. Recommendation.—Agreement should be reached as soon as possible on a "single scope" background investigation for all Top Secret and SCI clearances. The uniform policy should provide for: (a) less costly and more timely background investigations and clearances; (b) highest priority for meeting the five-year reinvestigation requirement; and (c) a subject interview in all cases.

49. Recommendation.—Government-wide adoption should be considered for the Stilwell Commission recommendations to prohibit the practice of requesting security clearances solely to provide access to a controlled area, where there is no need to know or even to be exposed to classified information. Reliability investigations should still be conducted in such cases, with standards equal to those proposed by this report for Secret clearances.

50. Recommendation.—More effective means should be established for investigating and clearing immigrant aliens and foreign nationals overseas who are granted access to classified information.

51. Recommendation.—Implementation of the proposal for one-time, short duration access by cleared personnel to the next higher level of classified information should be postponed until Secret clearance requirements and investigations are upgraded and the IG-CM(P) has reviewed the issue.

52. Recommendation.—The Executive branch should study the possibility, in consultation with appropriate congressional committees and civil liberties experts, of a program for requiring those who receive access to the most sensitive information to agree to expanded post-access foreign travel reporting obligations and/or agency access to relevant financial and travel records. Such a program would need to be clearly limited and to incorporate proper safeguards regarding the use of the information obtained.

53. Recommendation.—The National Strategic Security Program should increase personnel security research, including expanded research and evaluation on the wider use of psychological testing in the clearance process, taking full account of individual rights, as well as the implications of recent espionage cases.

54. Recommendation.—The President should issue a new Executive Order on personnel security. The order should provide for government-wide minimum standards and procedures and a policy oversight office similar to the Information Security Oversight Office. It should focus exclusively on personnel security programs regarding access to classified information and to sites where classified information is maintained. Drafting of this order should not delay action on other recommendations.

55. Recommendation.—The National Strategic Security Program should improve the adjudication process for granting or denying security clearances, with more rigorous standards regarding persons who have committed felony offenses; follow-up measures where persons with admitted problems like drug use are cleared; and a government-wide requirement for training of adjudicators. For the most sensitive positions, a "select in" policy based on demonstrated aptitude for security should be adopted in place of the current "select out" policy based on the absence of proved disqualifying factors.

56. Finding.—Agency and interagency investigations of recent espionage cases have highlighted flaws in hiring, assignment and termination practices. Recent corrective efforts in CIA and DoD and proposed government-wide consideration of similar measures should be very useful. The Committee will continue to monitor these efforts to achieve needed corrective action without destroying necessary managerial flexibility.

57. Recommendation.—The national Strategic Security Program should ensure full coordination of departmental policies and practices for the use of polygraphing in personnel security screening so as to maintain stringent quality controls and safeguards for individual rights, to prevent over-reliance on this technique, to provide for necessary research and funding, and to improve understanding of the procedures.

58. Recommendation.—Congress should consider permanent legislation authorizing DoD to use polygraph examinations for personnel security screening with CI-related questions, based on the most recent DoD proposal. If a decision cannot be reached in 1987 because of insufficient test data, then Congress should extend the current test program for a fixed period.

59. Recommendation.—The other Stilwell Commission recommendations on personnel security should be implemented vigorously in DoD with augmented OSD policy oversight, and they should be reviewed at the NSC level for adoption government-wide.

C. INFORMATION SECURITY

In December, 1985, the Committee submitted to the National Security Council a series of recommendations on information security, in response to a request for input on proposals developed by the Information Security Oversight Office (ISOO). In addition to calling for a National Strategic Security Program, as discussed above, the Committee urged immediate implementation of the ISOO proposals with strong, public endorsement of the President and the principal members of the National Security Council. The ISOO proposals would establish new information security policies for curbing over-

classification and over-distribution, improving classification management, enforcing the need-to-know principle, and improving security awareness and investigations of unauthorized disclosures. The Committee recommended that senior executives and program managers be held personally responsible for effective implementation of these policies.

Although the ISOO proposals are an excellent agenda for near-term actions, the Committee made several other recommendations for long-term decisions. First, there is a fundamental problem with the classification system because of its complexity. The Committee recommended consideration of a two-level system, based essentially on the current Secret standard and the Sensitive Compartmented Information model used in the Intelligence Community. A two-tier system offers a better chance of enforcing the need-to-know principle and reversing the natural incentives to over-classification.

The Confidential classification should be dropped, with such information either kept unclassified or protected at the Secret level. The initial decision should be whether the information requires protection in order to prevent substantial harm to identifiable national security interests.

The classification threshold should reflect a policy that classifies information only where truly necessary to maintain the national security. The report on Scientific Communication and National Security, issued in 1982 by a panel of the National Academy of Sciences, warned that undue controls can "weaken both military and economic capabilities by restricting the mutually beneficial interaction of scientific investigators, inhibiting the flow of research results into military and civilian technology, and lessening the capacity of universities to train advanced researchers." The 1985 interagency report on Soviet Acquisition of Military Significant Western Technology reiterated the warning that restricting access to scientific data "may also inhibit the United States' own national research effort." As stated recently by former DIA Director Eugene F. Tighe, "[I]f the U.S. security system for handling classified material is to be useful, only data that are critical to the United States' status as a political, economic and military power should be classified." The assumption should be that information is unclassified, unless there is a specific reason for maintaining secrecy.

The higher of the two classification standards should focus on the much smaller universe of data that require special protective measures above and beyond the normal safeguards for classified information. As is the case with intelligence data designated SCI, classification at the second level should be based on a full analysis of the risks of compromise. Such analysis should ensure that special protective measures are imposed only where necessary and are not diluted by applying them too widely. Careful analysis should also provide the elements for more effective security briefings that help senior policy-makers as well as lower level employees understand the consequences of a security breach.

Executive branch officials have noted that many bilateral and multilateral national security agreements are linked to the current system, and that the handling of Confidential-level foreign material at the Secret level will require some investment. The Committee recognizes that this change must be gradual. It is confident, howev-

er, that the declassification of many U.S.-generated documents that do not merit serious protective efforts will result in significant overall savings that can be devoted to better protection of Secret and Top Secret information.

Another concern is that a higher classification threshold would make more documents accessible to people who request them, either directly or under the Freedom of Information Act. However, unclassified information of a sensitive character can be marked "For Official Use Only" to maintain a policy of not releasing such materials routinely or in response to non-FOIA requests. Concern about FOIA, moreover, should not dictate classification management policy, which should be geared to the most efficient protection against hostile intelligence access to truly important secrets. If a case can be made that specific types of unclassified, but sensitive, information should be exempted from the FOIA, Congress should consider appropriate legislation as has been done for certain kinds of Defense Department technical data. This would be in keeping with the report on Scientific Communication and National Security, which called for development of specific criteria to determine whether unclassified scientific research should be protected by means short of classification.

The other information security recommendations sent to the NSC by the Committee addressed the problem of disclosure of classified information to the news media. The Committee is especially concerned about leaks that compromise sensitive intelligence sources and methods. The Committee emphasized the ISOO recommendation that more effective, unclassified educational materials be developed to explain the damage caused by unauthorized disclosures. The more important recommendation was for new procedures for authorized disclosure of classified information to the news media.

The Committee recommended that the NSC confront the pervasive practice of authorized disclosure of classified information on background, without permitting attribution to the source. By executive order, the President should require each agency to establish procedures to be followed whenever an official authorizes the disclosure of classified information to the news media or in any other public forum. The procedures should apply not only to formal statements for attribution, but also to disclosures on background. They should require that a decision be made to declassify the exposed information or that a record be maintained for purposes of accountability when authority is exercised or granted to disclose information that remains classified. The procedures should require consultation with the agency that originated the information and written designation of the officials in each agency who are authorized to communicate classified information to the media, either in person or through an authorized representative.

Some Executive branch officials oppose such procedures as likely to open the floodgates for "authorized leaks." Others want strict enforcement of a policy that any classified information disclosed to the media be officially declassified. The Committee strongly encourages adherence to a policy that officials speak on the record to the maximum extent. Nevertheless, there may well be valid reasons for retaining a background briefing's classified character. Any serious

effort to address the problem of leaks must face the realities of press-government relations. More leak investigations may accomplish little, moreover, so long as authorized background disclosures continue to divert investigators from cases in which administrative discipline, dismissal or legal action is possible. Policies that ignore "authorized leaks" simply reinforce the climate of cynicism that has fostered disrespect for security.

In addition to the recommendations submitted to the NSC in December, 1985, the Committee has several other information security recommendations. Many proposals of the Stilwell Commission on managing and controlling classified information should be considered government-wide. These include recommendations to:

Require, rather than simply permit, challenges to classifications believed to be improper.

Require a higher minimum degree of accountability for Secret documents.

Impose better controls over reproduction equipment used to copy classified information.

Initiate long-term action to develop technical or mechanical controls over unauthorized reproduction.

Reduce unnecessary retention and storage of classified documents.

Prohibit employees from working alone in areas where Top Secret or similarly sensitive materials are in use or stored.

The Stilwell Commission recommendations on special access programs and on National Disclosure Policy for transfers of classified information to foreign governments are particularly important.

The proliferation of special access programs is testimony to the failure of the current security system. ISOO Director Steven Garfinkel testified that "a number of these programs are probably unnecessary," and the Stilwell Commission reported that some actually afford less security protection than ordinary classification requirements. This situation reflects the fact that, too often, there is no real analysis of the hostile intelligence threat to special access programs or of the reasons why normal security standards and procedures offer inadequate protection. As the Stilwell Commission comments:

> [A]lthough the sole rationale for the creation of Special Access Programs under Executive Order 12356 is to provide enhanced security, there is sometimes too little scrutiny of this determination at the time such programs are created. Unless an objective inquiry of each case is made by the appropriate authorities, the possibility exists that such programs could be established for other than security reasons, e.g., to avoid competitive procurement processes, normal inspections and oversight, or to expedite procurement actions.

The Stilwell Commission's proposed policies, standards and controls for special access programs should be adopted government-wide. The development of minimum security standards for all DoD-established special access programs, which was recommended by the Stilwell Commission and has now begun, should end the temptation to use SAPs as a way to avoid normal security requirements.

The assignment of Defense Investigative Service personnel to work full-time at major contractor facilities may reduce the likelihood of problems like those recently revealed at Lockheed regarding protection of information on stealth technology.

Executive Order 12356 on National Security Information should be modified, moreover, to place more controls on the establishment of special access programs and to give the ISOO Director greater authority to conduct oversight and ensure accountability of special access programs. A revised executive order should designate the Secretary of Defense as the sole official entitled to create or continue defense-related, non-intelligence special access programs. There should also be a comprehensive, one-time review and revalidation of all existing special access programs and associated contracts, with each department and agency reporting the results to the ISOO Director who should make an independent assessment for the NSC.

The Committee believes ISOO has made a valuable contribution to better information security, but its small size (10 professionals) unduly limits its ability to conduct oversight inspections and other in-depth evaluations. ISOO's staff should be expanded to include a permanent element to inspect agency practices at all levels of command and management. While ISOO cannot replace internal inspections, it should do more to ensure the effectiveness of agency inspections by sampling on a periodic basis. ISOO should also work closely with the Defense Security Institute to implement the government-wide policy (proposed by ISOO) requiring seminars and training courses for all levels of commanders and managers, in government and industry, to understand information security policy and procedures, especially classification management.

Classification management training should focus, in part, on the fact that the only valid national security reason for classifying information is that a hostile element whose goal is to damage the interests of the United States should not have use of the information. Throughout the government, most classification judgments are made by the "proponent," i.e., the originator or functional manager responsible for the substance of the information. Few classification authorities consider or have a good knowledge of how a hostile element, government or otherwise, would use a particular piece of information to damage U.S. national security interests.

An informal query of government and industrial managers by Committee staff tends to validate the report that managers are often deficient in their knowledge of classification management requirements and procedures. The proliferation of classified documents and the need for greater security has sprawned an entire dictionary of special classification markings and control systems. The rise of these special markings and control systems has tended to generate a false sense of security and also to confuse those who do not fully understand their meanings. ISOO and the DCI should undertake a thorough reassessment of these practices with a view to simplifying the special markings systems.

Special markings help to enforce need-to-know restrictions by warning a reader what accesses are required to read a document. Equally important, however, is a need for clear assignment of responsibility for determining whether someone has a requirement

for access to information about a particular program. ISOO should review current directives and regulations to ensure that such responsibilities are pinpointed and that compliance is audited regularly.

Finally, the Committee does not believe that legislation to enhance criminal enforcement remedies for unauthorized disclosure of classified information would be appropriate this year. After completion of the appeals in the *Morison* case, a reassessment by both Congress and the Executive branch might be in order. The Committee does, however, support continued investigation of unauthorized disclosures within agencies and by the FBI for purposes of administrative discipline as well as criminal prosecution. When Department of Justice guidelines for leak investigations are reviewed pursuant to ISOO's proposal, they should be revised to reflect this policy. Polygraph examinations should also continue to be used in leak investigations on a voluntary basis in accordance with procedures followed in other types of criminal investigations.

Findings and Recommendations

60. Recommendation.—The Executive branch should immediately implement the Information Security Oversight Office (ISOO) proposals, with strong public endorsement by the President and the principal members of the National Security Council.

61. Finding.—The complexity of the current information security system has led to overclassification, employee confusion and ignorance, inability to protect all the information earmarked for protection, and, at least at times, cynical disregard for security.

62. Recommendation.—The Executive branch should consider simplifying the classification system by establishing two levels, eliminating the current Confidential classification. This streamlining should be preceded by consultation with other countries with whom the United States shares security classification agreements.

63. Recommendation.—An Executive Order should be promulgated requiring each agency to establish procedures governing authorized disclosure of classified information to the news media, including background disclosures of information that remains classified. Such procedures should require records for accountability, consultation with originating agencies, and designation of officials authorized to disclose classified information to the media.

64. Recommendation.—The Executive branch should review the Stilwell Commission proposals on managing and controlling classified information for possible government-wide implementation as part of the National Strategic Security Program.

65. Recommendation.—Executive Order 12356 should be modified to require greater controls on special access programs and to give the ISOO Director greater authority to oversee such programs. The Secretary of Defense should have sole authority to approve defense-related, non-intelligence special access programs. The whole government should conduct a comprehensive review and revalidation of all existing special access programs and associated contracts, with an independent assessment by the ISOO Director. Such reviews should be repeated on a periodic basis.

66. Recommendation.—ISOO's staff should be expanded to include a permanent inspection element. ISOO should work with the

Defense Investigative Service to implement improved training courses on information security and classification management. ISOO and the DCI should also reassess special markings with a view to simplification. ISOO should ensure that agencies designate individuals/positions with responsibility for determining need-to-know access.

67. Recommendation.—The Executive branch should postpone consideration of new criminal penalties for unauthorized disclosure until after the appeals in the *Morison* case. The Committee supports continued internal agency and FBI investigations for purposes of administrative discipline as well as prosecution, including use of voluntary polygraph examinations under criminal investigative procedures. Justice Department guidelines for leak investigations should be revised to reflect current policy of using administrative sanctions when prosecution is not pursued.

D. COMMUNICATIONS, COMPUTER, AND EMANATIONS SECURITY

The rapid expansion of electronic systems and equipment capable of very high-speed transmission and storage of large volumes of information offers striking capabilities and opportunities for the United States, particularly in the areas of national defense and intelligence. Equally striking are the security vulnerabilities of such systems, for which Executive branch efforts to develop and implement countermeasures are in their embryonic stage. The Defense Department and NSA have been given the lead in developing national policy for security countermeasures against hostile intelligence efforts to intercept communications, penetrate computer systems, and monitor the emanations from communications and information processing equipment.

Traditionally, communications security meant the encryption of classified communications and the maintenance of discipline to ensure that classified information was not discussed on open lines. In the 1970s, two weaknesses with this approach came to be recognized. First, it was discovered that the Soviets had a massive capability to intercept communications that could be exploited for significant intelligence value, even if the discussions were unclassified.

The second factor was the inherent human weakness of government and contractor officials, at all levels, who inevitably fail to follow strict security rules. The inaccessibility or inconvenience of secure phones, and the ease of slipping into or "around" sensitive topics, meant that security briefings and penalties were simply not adequate to prevent discussion of classified information on open lines.

Congressional concern about communications security has increased with growing public awareness of the threat. In 1985, Congress enacted Senator Moynihan's proposal that the FBI submit a report to Congress on the measures needed to counter the Soviet surveillance threat to domestic communications. This report was submitted in June, 1986, but was limited to the FBI's counterintelligence support role without discussing steps being taken or planned by the National Security Agency's Information Security Directorate to deny the Soviets access to domestic communications.

The NSA communcations security program is described in detail in the annual budget justification submitted to the Intelligence Committee for the first time in 1985. NSA has recently initiated a major program to upgrade communcations security by developing a low-cost, user-friendly secure telephone system. NSA's leadership in working with private industry to develop such a system may lead to a significant security breakthrough. NSA's plans to work with the private sector by licensing use of essential cryptographic techniques in equipment marketed to the public are unprecedented, and the Committee is satisfied with the efforts to take all equities into account. The Committee supports NSA's plans for secure telecommunications equipment, including the idea of making the equipment available to the private sector; it recommends attention at the highest levels to the need for agencies outside the traditional national security arena to join in this program as appropriate. The Committee will continue to exercise budgetary and policy oversight of NSA's communications security program.

In this regard, the NSA is concerned that current plans do not fully respond to the threat to long-distance communications relayed over satellite links and intercepted from sites like the one in Cuba. While the low-cost secure equipment developed under NSA's leadership may solve much of the problem for government agencies and private firms that can afford the cost, many organizations are much less likely to be able to pay the price. Efforts to neutralize the Soviet intercept operations that damage national security should not depend so heavily on the marketplace. Senator Moynihan, former Vice Chairman of the Intelligence Committee, has proposed a $1 billion program to encrypt all domestic communications satellite links. The Committee has asked for and received a five-year NSA plan to protect the most sensitive links that the Soviets could exploit to damage U.S. security interests. This less expensive proposal is to encrypt all dedicated channels leased by federal government agencies, by private firms with government contracts, and by private firms that communicate large financial transactions and economic forecasts. The Soviet could exploit these unclassified links by piecing together information that, taken in aggregate, is highly damaging to the United States. In the Intelligence Authorization Act for FY 1987, the Committee recommends an increase of $129 million for the communications security program above the funds requested by the Administration. More than half of this increase is to begin implementation of the domestic satellite protection plan.

Another threat comes from hostile intelligence efforts to monitor emanations from equipment and/or electrical lines. This problem generally bears the label Tempest, from the term used for the costly shielding and equipment design measures sometimes needed to ensure against compromising emanations. Improvements are being made in definition of the threat and the most cost-effective countermeasures. The initial security standards developed by the Defense Department and the Intelligence Community were based primarily on the theoretical possibility of compromise. A 1983 interagency assessment of actual and probable threats led to refinement of the threat assessment, since the current threat appears much greater abroad than in the United States. The bulk of Tem-

pest expenditures, however, is still being made in the United States.

On June 27, 1986, the General Accounting Office completed a review of domestic DoD and military service adherence to national Tempest policy for the House Committee on Government Operations. The GAO concluded that more than a year after the issuance of the new January, 1984, Tempest policy, the services all continued to follow their older internal Tempest guidance.

The GAO is of the view that the imposition of "Tempest countermeasures on industry should be controlled from a central point within DoD." Also in order to minimize unnecessary Tempest-related expenditures, the report recommends that the Secretary of Defense require all DoD components to conduct Tempest evaluations before implementing Tempest countermeasures in the United States to protect non-SCI information. Both the Stilwell Commission and an interagency body have recommended increased efforts to relate more closely the extent of the Tempest protective effort in the U.S. to the identified hostile collection threat. The expenditure of funds and effort for unnecessary Tempest protection clearly shows the need for better threat analysis and interagency collaboration in developing the communications and computer security aspects of a National Strategic Security Program.

The Committee sees a similar imbalance in resource allocation in the computer security field. Testimony at Committee hearings indicates a disparity in resources between the technological and human sides of the computer security problem. The overwhelming emphasis today is on increasing expenditures for development of more secure equipment and software, rather than on the personnel and information security measures needed to deal with the human side of the problem. The DCI testified that personnel security is "the most important part of any effective security program," yet the Computer Security Center at NSA and the interagency computer security committee (under the National Telecommunications and Information Systems Security Committee chaired by the Assistant Secretary of Defense for C^3I) have focused mainly on hardware and systems design.

The Stilwell Commission, citing the estimate that redressing the damage from the Walker-Whitworth case could cost several billion dolars, went on to warn:

> Given the range of density of information housed in major DoD computer-based systems, the possibility of remotely accessing terminals over great distance, and the difficulty of detecting exploitation by a trusted person, it is entirely conceivable that a computer-wise traitor could cause catastrophic loss of resources and military advantage.

The security officer for one of the larger military logistics computer systems sites expressed the same concern to Committee staff. The Committee is also concerned about the apparent use of a DoD computer system in a scheme to divert parts to Iran.

The trusted-person threat to computer security is not limited to the Defense Department. The State Department has a problem due to the fact that many embassy computer system managers and operators are foreign nationals. In light of the sensitivity of even un-

classified State Department systems, Members of the Committee sponsored an amendment to the Diplomatic Security Act to protect funding for State Department initiatives to replace those personnel with U.S. citizens.

Because of the seriousness of the computer security threat, the Committee urges consideration of the option suggested in a 1985 interagency assessment: "The only recourse may be for the United States to exclude from these data bases the types of science and technology information that are likely to be used against U.S. interests." The National Strategic Security Program should ensure that the computer security and information security communities jointly develop procedures requiring analysis of computer system vulnerabilities before sensitive material is approved for storage in those systems.

Given the gravity of the personnel security problem, the National Strategic Security Program should address the need for more stringent controls on personnel with access to sensitive computer data bases. As a result of the Walker-Whitworth case, special "crypto-access" controls have been approved for personnel with extensive access to classified cryptographic information. Similar controls should be considered for access to the most vital data bases and networks. Furthermore, such positions should have top priority for institution of personnel reliability program measures, as recommended by the Stilwell Commission for DoD personnel involved in especially sensitive programs.

One reason for the apparent imbalance in attention to technological and human aspects of the computer security problem may be the national policy structure that separates communications and computer security from other security functions. In 1984 the President issued NSDD–145, which made NSA the "national manager" for communications and computer security under a new National Telecommunications and Information Systems Security Committee (NTISSC) chaired by the Assistant Secretary of Defense for C3I. NSDD–145 was an important effort to update national policy, because it recognized the close connections between computer and communications security. The Committee endorses the assignment of NSA, working through its National Computer Security Center, to conduct research and develop computer security hardware, systems and standards not only for DoD, but also for the federal civilian establishment and segments of the private sector. The National Bureau of Standards Institute for Computer Science and Technology is cooperating with NSA in transmitting research results throughout the government and to private industry. These efforts should increase.

Computer security is, however, one of the best examples of why a still broader national policy structure is essential to ensure full attention to all aspects of security counter-measures. While NSA has unique technical capabilities, computer security priorities should be addressed as part of the National Strategic Security Program to ensure that research efforts and resource allocation respond to the most serious actual and probable threats. (Another reason for a framework spanning current jurisdictional divisions is that TEMPEST issues relate closely to technical surveillance countermeasrues, as discussed below.)

Recently, fears have been expressed regarding a "big brother" role in NSA's growing involvement with the civilian and private sectors. The Committee believes that NSA is best equipped to develop technical measures needed to remedy serious vulnerabilities in a timely manner. The Committee also recognizes that both the Executive and Legislative branches must continue to exercise oversight to ensure that the Government does not impose technical solutions that impinge on individual privacy, civil liberties or public confidence.

To improve congressional oversight of resource allocation, program priorities and privacy concerns, the Committee instituted a review of the NSA communications and computer security budget requests beginning with FY 1987. The House Intelligence Committee began this practice last year, and the funds were included for the first time in the Intelligence Authorization Act for FY 1986. While these NSA programs are not part of the National Foreign Intelligence Program and thus are within the concurrent jurisdiction of the Armed Services Committee, they also fall under the Intelligence Committee's general mandate in Senate Resolution 400 for oversight of measures taken to protest against the hostile intelligence threat.

Findings and Recommendations

68. Recommendation.—The National Strategic Security Program should ensure that NSA's plan for low-cost, secure voice telephone equipment is implemented by all government agencies, contractors and offices involved with national security information and other technological, political and economic information of significant value to adversaries.

69. Finding.—A program for encryption of domestic commercial communications satellite links that would be the most lucrative targets for hostile interception of private communications is a worthwhile supplement to the secure phone program. The Committee has recommended FY 1987 funding to begin this program.

70. Recommendation.—The National Strategic Security Program should enforce current national TEMPEST policy for all government agencies, so that decisions to buy TEMPEST equipment are based on the best counterintelligence estimates of actual and probable threats.

71. Recommendation.—The National Strategic Security Program should place greater emphasis on personnel, physical and information security aspects of computer security, including research efforts, and should establish relative priorities for all aspects of computer security countermeasures.

72. Finding.—Because U.S. embassy computers and word processing systems may contain sensitive information, Committee Members sponsored an amendment to the Diplomatic Security Act to protect State Department funds to place U.S. citizens in charge of embassy computers.

73. Recommendation.—The computer security and information security communities should review and improve current procedures for analysis of information system vulnerabilities before sensitive material is approved for storage in such systems.

74. Recommendation.—Given the gravity of the threat, high priority should be given to strict personnel security controls, comparable to the reinstituted crypto-access program and incorporating personnel reliability programs, for persons with extensive access or potential access to sensitive computer systems.

75. Recommendation.—The National Strategic Security Program should provide for national-level review of communication, computer and emanations security resource requirements, with NSA continuing to be responsible for development of technical measures and standards needed to remedy vulnerabilities. The Committee will continue to oversee the level of effort and to ensure that technical measures are not imposed in a manner that impinges on individual privacy, civil liberties or public confidence.

E. TECHNICAL AND PHYSICAL SECURITY

In June, 1985, the Committee heard detailed testimony on the bugging of typewriters at our Moscow embassy and other Soviet technical surveillance operations. This testimony vividly demonstrated the Soviets' strong technical surveillance capabilities and U.S. vulnerability to sophisticated electronic penetration and eavesdropping techniques. Shortly thereafter, the Inman Panel on Overseas Security submitted to the Committee a compartmented annex to its report to the Secretary of State, showing that the technical security threat is a formidable challenge. The Inman Panel stressed fundamental problems for the State Department and recommended both a reorganization of State Department security operations into a new Diplomatic Security Service and a massive rebuilding program for overseas missions. The Moscow embassy discovery and the Inman Panel report have reawakened the intelligence community and the State Department to the threat of hostile technical surveillance.

The Committee recognized after the June, 1985, hearing that U.S. technical surveillance countermeasures (TSCM) had been seriously underfunded in recent years. Consequently, the Committee proposed what became a $35 million FY 1985–86 supplemental appropriation to enhance security countermeasures at U.S. facilities abroad.

The physical security lapses that allowed Soviet access to State Department equipment and the low funding for technical surveillance countermeasures are matters of grave concern to the Committee. As a result, the Committee accompanied its proposal for a supplemental appropriation with a request for a comprehensive long-range plan for upgrading technical security at U.S. facilities abroad. The outlines of such a plan are beginning to take shape.

The Committee is pleased to note the cooperation and progress achieved in this area by Executive branch agencies in 1986. The best way to marshal their energies is, however, to establish a National Strategic Security Program that can take all interests and disciplines into account. Current interagency mechanisms will benefit from being incorporated in this broader and more formal framework. This recommendation is consistent with an interagency assessment that emphasizes the necessity for total protection of information and telecommunications equipment and with the testi-

mony of CIA's Security Director that "the best security will be achieved through a program that integrates technical security with other security disciplines."

Many agencies play R&D or operational roles in detecting and denying technical penetration by hostile intelligence services. Adequate TSCM planning must do more than just provide an organizational framework and philosophy. It should outline explicitly the vulnerabilities, requirements, objectives, responsibilities, resources and schedule for short and long-term R&D, training, personnel, inspection and other needs. The Committee looks forward to this level of effort in the future.

Implementing the Inman Panel recommendations, the State Department has established a new Diplomatic Security Service so as to give those who manage its security functions higher status, increased resources and a greater voice in Department management. State has also developed a $285 million construction plan to build more secure facilities in Eastern Europe. The State Department is establishing programs, moreover, to ensure that all information processing equipment sent abroad is under strict security controls. These efforts are a sensible response to the vulnerabilities uncovered by the discovery of the bugged typewriters. The Committee has encouraged development of this program, and Members sponsored an amendment to the Diplomatic Security Act that protects funds for it.

Congress should also support the substantial, multi-year expenditures that will be required to implement Inman Panel recommendations for enhanced physical security at U.S. facilities overseas. Congress funded initial requests to improve embassy security against terrorism, including President Reagan's request for a $110.2 million supplemental appropriation for FY 1985 and the Act to Combat International Terrorism (P.L. 98–533), which authorized $366.3 million for embassy security. The urgent supplemental for FY 1987 appropriates over $700 million to begin the new construction and other security enhancements.

The Committee understands that there must be a "rule of reasonableness" in embassy physical security that takes into account the need for openness and the negative effect of a "fortress" image. Nevertheless, policy and design should be flexible enough to respond not only to the terrorism threat, but also to the hostile intelligence threat.

Security expertise in other agencies can contribute significantly to the success of the embassy construction program and it will be important to factor technical security requirements into both the planning and the construction of new facilities. This Committee has worked closely with the Senate Appropriations Committee to provide funds and positions in the FY 1987 urgent supplemental for such assistance to the Foreign Buildings Office of the State Department.

The State Department advises that budget constraints have required modification of the plans for certain construction which originally would have made necessary security improvements in FY 1988. The revised plan stretches out construction work through FY 1990. The Committee urges the Administration to accelerate its

decisions in light of long-range, tailored security plans for each of these missions.

Findings and Recommendations

76. Recommendation.—The Executive branch should continue to place greater emphasis on the development of means and the implementation of actions to detect and defeat technical penetrations of sensitive facilities. The National Strategic Security Program should reconcile the various technical security interests and integrate them with other security disciplines.

77. Finding.—Executive branch actions in 1986 to upgrade security functions and to coordinate technical security efforts have been a notable step forward. They deserve continuing high-level support and resource commitments.

78. Finding.—State Department plans to improve the security of information processing equipment constitute a reasonable approach to the technical penetration problems. Committee Members have moved to ensure that the needed funds to begin these programs are available.

79. Recommendation.—Congress and the Executive branch should support implementation of the Inman Panel recommendations for major site and/or physical changes to U.S. facilities abroad to enhance security, minimize acts of terrorism and prevent hostile intelligence penetration.

80. Recommendation.—The State Department should ensure that security experts in other agencies are given full opportunity to participate in the planning and oversight of new embassy construction efforts to achieve a comprehensive security system. Decisions on long-range, tailored security plans for overseas missions should be accelerated.

F. INDUSTRIAL SECURITY

Espionage cases of the past ten years, involving such industry personnel as Boyce, Lee, Bell, Schuler, Harper and Cavanagh and the loss of sensitive technological information through increasing levels of espionage and illicit transfer, have highlighted the priority that hostile intelligence services attach to U.S. technology. The interagency report in 1985 on Soviet Acquisition of Militarily Significant Technology described the threat, and its findings are confirmed both by Soviet documents obtained by the French and by the testimony of Soviet bloc defectors. Industry is vulnerable to recruitments by hostile services and to employees who volunteer their information for pay. Industrial communications are vulnerable to Soviet interception; and industrial facilities are susceptible to technical penetration, especially overseas. Co-production agreements with foreign firms compound the difficulties.

Hostile intelligence successes in penetrating U.S. industry, culminating in the Harper case, triggered an in-depth review of industrial security programs and policies in 1984 by a DoD Industrial Security Review Committee (also known as the "Harper Committee"). This review was particularly important because DoD has been delegated industrial security responsibility for eighteen federal departments and agencies. The Harper Committee's 25 recommendations

are designed to enhance industrial security dramatically. While not all have been adopted by DoD, the majority are being implemented as proposed or with some revisions. The Committee urges prompt action on the Harper Committee reforms that have been approved for implementation. The National Strategic Security Program should also review those recommendations for government-wide implementation.

Several Harper Committee proposals deserve special emphasis. First is better integration between counterintelligence and industrial security. In the past, there has been a reluctance on the part of the counterintelligence community to communicate with industrial security officers. While such communication is improving, particularly in security awareness programs such as the FBI's DECA program, there is ample room for closer cooperation. There should be a continous two-way sharing among counterintelligence agencies and government and industrial security officers. Counterintelligence agencies should provide more tailored information on the hostile intelligence threat to particular programs or types of programs, as well as in particular geographical areas, for use in security awareness efforts and the design of security measures.

A pilot program should be initiated for assignment of Defense Investigative Service personnel to large sensitive contractor facilities on a full-time basis, and the National Strategic Security Program should review the results as a basis for considering a similar government-wide practice. With 95 percent of all classified documents (an estimated 15 million out of 16 million) residing with only 4 percent of the cleared industrial contractors, the case for a continuing government security presence at those facilities is strong. It is further enhanced by the admissions of the Chairman of the Board of Lockheed regarding the sloppiness of the company in accounting for classfied documents. A GAO investigation had revealed that Lockheed was unable to account for nearly 1,500 documents due to inadequate controls. A reordering of priorities to concentrate on major contractors will not result in the government taking over contractor security functions, but rather will permit timely audits of security functions and correction of problems in primary facilities.

As discussed in the section on personnel security, a single-scope background investigation for Top Secret and SCI clearances would especially benefit industrial security. The five-year goal for clearing up the backlog of periodic reinvestigation for Top Secret and SCI, if applied government-wide, would similarly benefit contractors who are on the leading edge of U.S. intelligence technology. The Committee has added funds to agency budgets for this purpose on more than one occasion.

Industrial security managers have had to cope with tremendous needs for, and resultant delays in, clearance investigations for industry. With the large defense buildup in recent years has come a dramatic rise in the number of contractor personnel holding security clearances. Between FY 1978 and the end of FY 1985, the number of such clearance investigations per year increased from 28,000 to 75,000. The Defense Department's recent twenty-percent reduction in clearances should help ease this burden.

Federal Acquisition Regulations should be changed to designate security requirements for classified contracts as a direct cost. When security is designated as a direct cost instead of an overhead cost, industrial security officers are relieved of the opposing pressures of the government-customer who demands more and better security and the company officials who see security as a drain on profitability. In addition, the designation of security as a direct contract cost will force the customer to more precisely define his security requirements in the Request for Proposals (RFP) and in security deliverables. While this approach may appear more costly to the taxpayer, in the long run it will result in greater cost savings through effective planning and cost controls.

Consideration should also be given to the greater use of Cost Plus Award Fee (CPAF) contracts as an incentive for fulfilling contract security requirements and specifications on time, within cost and without security violations. Making security a major award fee determinant along with the other award fee elements will give contractors for classified contracts the motivation for ensuring that more and better-qualified security planning and operations personnel are assigned and retained on contracts.

Training and government certification of all current and planned contractor security officers should be required in each classified contract. As pointed out in the Harper Committee report, the intense targeting by hostile intelligence services of the large amount of classified data entrusted to contractors, as well as the absence of a formal training program for industrial security officers, justifies the government's establishment of this requirement. The requirement for training and certification should also apply to personnel with security responsibilities for special access program contracts.

A final and most disturbing concern is the hostile intelligence threat to foreign subsidiaries of U.S. firms and to foreign firms that have co-production agreements with the United States. Although U.S. counterintelligence efforts abroad, both unilateral and in concert with our allies, can help deal with this problem, it also requires national policymaker attention. The Stilwell Commission warned specifically of the critical problem with co-production arrangements, "where losses could entail not only the end-item being produced but also the technical 'know-how' necessary to manufacture it in large quantities." Other weaknesses identified by the Commission include insufficient controls in the sale of classified weapons systems and ineffective security surveys. The Committee fully endorses the Stilwell Commission's recommendations for improving the National Disclosure Policy, which governs transfer of classified military information to foreign recipients. The following approach would be required in approving classified transfers:

(1) requiring a determination that the need of the recipient cannot be satisfied by unclassified systems or data;

(2) if classified systems or data are required, then requiring selection of a model or type of such system that minimizes the need to transfer classified information;

(3) requiring phasing in of the most sensitive classified information over time, if feasible;

(4) avoiding co-production of military systems which involve the manufacture of the most advanced version of classifed components or end-items.

In addition, security surveys would be conducted by a permanent professional staff with flexibility to meet pressing needs for in-country security assessments. The National Strategic Security Program should ensure that such improvements are implemented not only for military information, but for sensitive intelligence and nuclear matters as well.

Findings and Recommendations

81. Recommendation.—The National Strategic Security Program should foster better communication between U.S. counterintelligence agencies and industrial security officials and provide more tailored information on the hostile intelligence threats to particular programs or areas.

82. Recommendation.—DIS should initiate a pilot program for assignment of its personnel to large sensitive contractor facilities on a full-time basis, and the results should be reviewed as a basis for a similar government-wide practice.

83. Finding.—Recently adopted goals for ending the reinvestigation backlog for contractors holding Top Secret and SCI clearances who are currently involved in sensitive classified contracts merit high-level commitment and support.

84. Recommendation.—Federal Acquisition Regulations should be changed to designate industrial security for classified contracts as a direct cost. The primary intent of this proposal is to identify and monitor security costs associated with particular contracts.

85. Recommendation.—Consideration should be given to greater use of Cost Plus Award Fee contracts as an incentive for fulfilling contract security requirements.

86. Recommendation.—Trained and government-certified security officers should be required in each classified contract, including those for special access programs.

87. Recommendation.—The National Strategic Security Program should ensure implementation of the Stilwell Commission recommendations on National Disclosure Policy not only for military information, but for sensitive intelligence and nuclear matters as well.

88. Recommendation.—Other Harper Committee recommendations approved by DoD should be implemented promptly and reviewed for government-wide application.

G. CONGRESSIONAL SECURITY

In December, 1985, Randy Jeffries, an employee of a private firm that transcribed classified hearing transcripts for congressional committees, was arrested for attempting to sell classified material to Soviet intelligence. The FBI detected the employee making contact with the Soviet Military Office in Washington. The employee admitted giving the Soviets excerpts from a classified transcript of a House Armed Services Subcommittee hearing on Defense Department command, control, communications and intelligence programs. The subsequent FBI investigation revealed that the employ-

ee had been observed by a co-worker removing classified documents from the firm under his coat and that a friend of his had destroyed a locked briefcase given to him that possibly contained classified documents. Jeffries pleaded guilty in January, 1986, to a charge of supplying national security documents to a person not entitled to receive them. This offense carries a maximum sentence of ten years in prison.

The case highlights the fact that Congress is not immune from the espionage problems that have surfaced throughout the government in recent years. Both Executive branch and congressional inquiries have emphasized the need to enhance congressional security in response to espionage threats. In November, 1985, the Stilwell Commission expressed the following concerns about the handling of classified information by Congress:

> [A]lthough Executive Order 12356 provides that departments and agencies may disseminate classified information to persons outside the Executive branch provided such information is given "equivalent protection" by the recipient, DoD elements frequently provide classified information to the Congress without any understanding of how such information will be protected. While all congressional staff members who receive access to classified DoD information are, in theory, cleared by DoD, little attention is given the handling and storage of such information by congressional staffs, who are not, in fact, bound by the safeguarding requirements of Executive Order 12356.

The Stilwell Commission recommended that the Secretary of Defense take the following actions:

> Urge the President of the Senate and Speaker of the House of Representatives to adopt, for each House of Congress, rules to provide uniform minimum control over classified information provided by departments and agencies of the Executive Branch. Volunteer to provide DoD resources and assistance to Congress to achieve this goal.

In January, 1986, the Report on the Federal Government's Security Clearance Programs by the Permanent Subcommittee on Investigations of the Senate Committee on Governmental Affairs addressed this subject in the following observation:

> Congress must also focus on problems dealing with classified information in the legislative branch. For the most part, there are no established standards and procedures. Personal offices and Committee practices vary widely in terms of their handling of clearances and classified material. There are few, if any, checks in this system. We believe an overall review of security procedures in the legislative branch should be conducted by the Rules Committee, in consultation with the Intelligence Committee, with a goal of recommending improvements where needed.

The Chairman and Ranking Minority Member of the Subcommittee, Senators Roth and Nunn, addressed this issue through preliminary letters to the Senate leadership.

The Senate Intelligence Committee has received information from the FBI and other U.S intelligence agencies regarding the operations of the intelligence services of Communist countries directed at Members of Congress and their staffs, including attempts to recruit or place agents in Congressional offices. Electronic surveillance of domestic communications by foreign countries also poses threats to Congress. Only a few congressional offices have secure telephones linked through the Executive branch system.

The information provided to the Intelligence Committee about the espionage threat to Congress indicates a continuing pattern of activity designed to exploit vulnerabilities in security. In three cases over the past ten years, the FBI has uncovered and disclosed publicly Soviet bloc attempts to recruit and place American citizens as agents inside Congressional offices. U.S. counterintelligence successfully prevented any damage in the following cases:

In 1976 a political scientist employed by the Atlantic Council, James Frederick Sattler, was revealed to be attempting to secure a position with a House Foreign Affairs Subcommittee, after being recruited and trained as an espionage agent by East German intelligence.

In 1980 a former CIA case officer, David Barnett, was prosecuted for espionage based on evidence that he had sold CIA information to Soviet intelligence and had attempted to gain employment with the Senate and House Intelligence Committees on the instructions of Soviet intelligence.

In 1982 a staff assistant to a House Member reported to the FBI an effort by Soviet intelligence to recruit him as an agent. At the FBI's request, the staff member became a "double agent" to learn more about Soviet intelligence techniques and aid U.S. counterintelligence.

In other cases, which have not been disclosed by the FBI, there is additional evidence of espionage targeting of Congress by Communist intelligence services.

In more general terms, the FBI has described the techniques used to penetrate the Congress. Communist countries assign intelligence officers to the United States as diplomats, journalists, trade representatives, and in similar capacities. Some of these intelligence officers are instructed to cultivate associations with Members of Congress and congressional staff for the purpose of developing confidential relationships. A well-trained intelligence officer knows how to approach individuals so as not to appear in any way hostile or threatening. Sophisticated and skillful intelligence officers can establish relationships that seem entirely innocent. Professional, academic or social contacts lead to friendships without any suggestion by the intelligence officer of anything illegal or improper. Only when the intelligence officer has learned enough about an individual's vulnerabilities will an effort be made to exploit the relationship.

Lax security practices offer greater opportunities for an intelligence officer to succeed in compromising a congressional staff member. Unlike Executive branch personnel, congressional staff have no requirement or established procedure for reporting contacts with representatives of Communist countries. In some cases,

Members or their staff do report such contacts to the FBI, but the record is very uneven.

The purpose of contact reports is to assist the FBI's investigations of suspected foreign intelligence officers. The FBI has advised the Intelligence Committee that its investigations of suspected intelligence officers disclose many contacts with individuals who, after further inquiries, are found to be congressional staff. Contact reports save the FBI much time and effort, as well as enabling it to advise staffers on how to handle such contacts. That agency has raised with the Intelligence Committee the need for a more formalized procedure in the Senate for briefing staff on the espionage threat and for reporting contacts with representatives of Communist countries.

Another matter that the FBI has discussed with the Intelligence Committee is the handling of classified documents in the personal offices of Members. The FBI has offered to develop both classified and unclassified briefings on the espionage threat to Congress from the intelligence services of Communist countries. The Defense Department, which is responsible for most of the security clearances for congressional staff, might be an appropriate source of assistance in briefing staff on the handling of classified materials.

In an effort to address issues related to Senate classified information security, the Senate Sergeant at Arms, in November, 1985, circulated a Senate Select Committee on Intelligence questionnaire to all Members' personal offices and Committees of the Senate. The results of that questionnaire were not encouraging. Based on responses from 60 Senators' offices, the following conclusions can be drawn:

There is confusion about the levels and sensitivity of the classified information received in personal offices.

There is no uniform procedure followed for storage or control of classified information in personal offices.

Staff with clearances in personal offices rarely receive security indoctrinations or other security education.

As a result of the security survey and the foreign intelligence threat to the Congress, the Senate Select Committee on Intelligence, together with the leaders of the Committee on Rules and Administration and the Committee on Governmental Affairs, determined that the key to addressing the Senate's information security problems lies in the creation of a central office within the Senate to develop and oversee much-needed standards and procedures on important personnel security and information security issues.

The security assistance that a central office would provide includes:

Receiving, controlling, transmitting, storing and destroying classified material.

Processing clearance requests for personnel of the Senate.

Maintaining a centralized record of clearances held by personnel of the Senate.

Presenting security briefings and debriefings for the benefit of Senate personnel.

Consulting on security issues with the personal offices and committees.

64-268 O - 86 - 4

Conducting administrative liaison with other U.S. Government agencies on behalf of the Senate.

A particularly troublesome question relating to classified information security is the large number of Senate staff having access to classified material. The Senate security office should be required by resolution to conduct a comprehensive survey of all Senate offices to determine which officers and employees hold security clearances. The director would report this information within 90 days to the Majority and Minority Leaders along with comments and/or recommendations as to the feasibility of reducing the number of Senate staff with security clearances.

Another early task of the proposed office should be to devise a Senate Security Manual whose provisions, if approved by an oversight group and the full Senate, would be binding on all Members, Officers and employees. The Committee has provided to the Senate leadership a draft Senate security manual to serve as a basis for discussion which is reprinted in Appendix G to this Report. The draft security manual contains standards and procedures both for the handling of classified information and for personnel security.

Findings and Recommendations

89. Finding.—Hostile intelligence services have attempted to penetrate the staffs of Senate and House Members and Committees. Hostile services use sophisticated techniques to develop contacts that can lead to intelligence recruitments.

90. Finding.—Lax security practices in the Senate increase the risk of compromising sensitive information. There is no requirement or procedure for reporting contacts with representatives of Communist countries. There are no established procedures for handling classified information, especially in Member offices. There is no accountability for the handling of such information, and there is great confusion about the sensitivity of the information and what should be done with it. There is no central point where the number of Senate employees with security clearances is tallied or where such services of common concern as security briefings and day-to-day information security assistance are provided.

91. Recommendation.—The Senate should establish a central security office to develop and oversee standards and procedures on important personnel security and information security issues.

92. Recommendation.—A central security office, once established, should immediately survey all Senate offices to determine which offices and employees hold security clearances. This information should be reported within 90 days to the Majority and Minority Leaders along with comments and recommendations on the feasibility of reducing the number of Senate staff with security clearances.

93. Recommendation.—The proposed office should develop a Senate Security Manual, the provisions of which would be binding on all Members, Officers and employees.

94. Recommendation.—All Members and employees of the Senate should be encouraged, and employees with security clearances required, to report contacts with Communist country officials or other suspected foreign intelligence officers. The central security

office should establish a procedure for such reporting, either through it or directly to the FBI.

95. Recommendation.—Further recommended items for consideration by the Senate security office include: establishment of a Senate corps of cleared employees for transcribing and reporting classified hearings; and improvement in the communications security of telephone conversations, classified computer data, and face-to-face discussions of a sensitive nature.

APPENDIXES

APPENDIX A

UNITED STATES DISTRICT COURT, NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, PLAINTIFF,

v.

JERRY ALFRED WHITWORTH, DEFENDANT.

Criminal No.: 85-0552 JPV

Affidavit of Rear Adm. William O. Studeman, Director of Naval Intelligence

1. I am William O. Studeman, a naval officer presently holding the rank of Rear Admiral. I was commissioned an Ensign in the Navy in 1963, and have served virtually continuously on active duty as a naval intelligence officer since that time. My present position is that of Director of Naval Intelligence, which I have held since September 1985. As Director of Naval Intelligence, I am responsible for the collection, analysis and distribution of intelligence information within the Naval Service. I am the Navy's sponsor for counterintelligence programs executed by the Naval Security and Investigative Command, under the policy auspices of the Office of the Secretary of Defense. I offer this affidavit to the Court for use as it deems appropriate in constructing an appropriate sentence for the defendant in this case.

2. The defendant in this case, formerly Senior Chief Petty Officer Jerry Alfred Whitworth, served the United States Navy for 24½ years, 18 of which were in the rate of Radioman, rising to the rank of Senior Chief prior to his retirement. The primary function of a Radioman is to provide and maintain the ability of Department of Defense and naval forces to communicate with each other as well as senior and subordinate commands. Unlike the navies of old, virtually all the information required to plan, operate, command, maintain, modernize, repair, replenish, warn, inform and control the military forces of all the services and our allies is exchanged electrically via communication systems, most of which are considered secure by virtue of their cryptographic cover. Electrical distribution of naval messages is an essential backbone activity designed to reach all levels of command in the Navy. This naval communications system is operated by some of our brightest people who are given the tools, training and sacred trust to protect the vital high technology systems and access to sensitive secrets which are placed

in their hands. It is important, therefore, to understand the vulnerabilities inherent in naval communications, to understand the concept of crytographic support to communications security (COMSEC) and to understand how Radioman Senior Chief Jerry Whitworth's violation of his trust as a member of the elite fraternity of naval communication professionals has resulted in unprecedented damage to the Navy and the nation.

3. Cryptographic systems are designed to encipher information so that only the holders of the system will be able to decipher that same information. Contemporary crypto-equipments accomplish enciphering and deciphering on the basis of complex mathematical formulas called "logic", which are designed as an integral part of the system with changeable additives called "key". To decipher an intercepted message, an adversary must know both the logic and the key of the cryptosystem used to encipher it. Since it is effectively impossible to ensure that the logic of a cryptosystem will not be compromised during the years it remains in effect, the security of our machine cryptosystems depends on ensuring the integrity of the associated key and the personnel who care for the system. "Key" literally will unlock the secrets contained in encrypted communications.

The ultimate vulnerability of cryptosystems and all procedures designed to protect sensitive information lies at the human level. For this reason, personnel chosen for communications-related duties are carefully screened and indoctrinated in the especially sensitive nature of the positions they hold and the fiduciary-like nature of the trust placed in them. No system ever designed can be invulnerable to the corrupt, cleared individual who has access to sensitive information. Thus, we depend on an individual's integrity and deterrence of the law to ensure that this trust is fulfilled.

4. The importance of key was amply demonstrated by the evidence in this trial. The Soviets were clearly willing to pay a high price for key—more than $300,000 for the defendant alone. But the price paid by the Soviets pales in comparison to its worth. Naval intelligence analysis has led us to conclude that the Walker-Whitworth espionage activity was of the highest value to the intelligence services of the Soviet Union, with the potential, had conflict erupted between the two superpowers, to have powerful war-winning implications for the Soviet side.

5. The importance of the individual spy cannot be overestimated in this type of intelligence acquisition. When an adversary covertly obtains the protective key supplemented by large volumes of actual messages, he can potentially read any or all intercepted messages which that key protects. In the case of Navy operational command circuits, this can be literally hundreds of messages per key setting, many of which are vital to the national security of the United States. Normally, the information contained in those encrypted messages could be expected to include, at a minimum, further plans, ship locations and transit routes, military operations, intelligence activities and information, weapons and sensor data, naval tactics, terrorist threats, surface, subsurface and airborne doctrine and tactics, and similar information which could prove of incalculable value to hostile powers. Undetected theft of cryptographic key by persons intent on penetrating COMSEC safeguards can have ex-

tremely dire consequence to the defense posture of the nation. History is replete with examples of the benefits and risks associated with COMSEC made vulnerable by espionage or otherwise penetrated for the benefit of one side or another. Such vulnerabilities sustained over time have altered the course of history and can do so again in the future.

6. With respect to this specific case, the sheer volume of encrypted data compromised to the Soviet Union makes it impossible to describe all of that data with specificity. The Court has already heard a few of the specifics during trial; therefore, in paragraphs 7-9, I will simply describe generically the types of information which have likely been traded to the Soviet Union through the years of this espionage enterprise. I will briefly mention some of the more significant aspects of the defendant's activities. I will also provide to the Court certain conclusions I have drawn concerning these compromises. My conclusions are based on my twenty-four years experience as a naval officer, as both a user and producer of intelligence information, and on my current responsibilities as Director of Naval Intelligence and the Senior Intelligence Officer for the Department of the Navy.

7. *Ship location and transit information.*—This is perhaps the most common type of information transmitted over naval communications circuits. On any given day the transit passages and locations of numerous naval vessels, both U.S. and allied, will be transmitted in encrypted radio traffic. Normally, this type of data is held confidential until the information is no longer valid. The reasons that ship locater information is temporarily classified are three-fold. First, simple prudence dictates that the location of ships of the line be held confidential while that sort of information can enhance their vulnerability. This is especially true during periods of hostility. For example, during the Vietnam era, compromises of this type of information could have been responsible for ineffective air strikes, downed aircraft, abandoned targets and infantry losses. It is also particularly true today when U.S. and allied vessels pose a lucrative target for terrorist attack. Secondly, the location and transit routes of naval vessels can be valuable information leading to disclosure, either directly or by informed analysis, of naval doctrine and tactics. This, in itself, could prove to be decisive to the outcome of an engagement at sea. Finally, the rationale that persuades the United States to maintain the confidentiality of ship movements is universally shared by allied nations. Disclosures of transit movements of our allied navies would be as potentially harmful to them as to our own ships; therefore, inappropriate disclosures of such information resulting from breaches of U.S. security could reasonably be expected to have some adverse impact on both foreign relations and on international military cooperation.

8. *U.S. Naval operations information.*—The volume of communications traffic concerning naval plans and operations is large. As with the previous section, analysis of naval plans and operations information can lead, either directly or by informed analysis, to disclosure of naval excerises, contingency activities, and future combat operations which can be exploited to the advantage of a hostile power. In addition, communications will invariably reveal classified technical information, intelligence data, intelligence sur-

veillance activities or information critical and potentially harmful to the foreign policy of the United States. It would directly reveal substantive information used by the United States in making decisions concerning the security of the nation and its foreign policy. If a hostile power were to obtain that information, it would be possible to turn this newly acquired information to the disadvantage of the United States, either by adopting measures to counter the advantage otherwise available to the United States, or by inserting misleading data into the collection process. An indirect benefit of obtaining this information would be the ability to analyze it for intelligence value, and to inferentially extrapolate the location and concentration of resources dedicated by the United States to obtaining similar information worldwide. Thus, disclosures of specific data can lead to harmful results, both for the specific collection activity involved, and also for similar activities conducted worldwide by U.S. forces and other agencies of the government.

9. *Special category (SPECAT) information.*—Frequently it is necessary to transmit information which is of such a degree of sensitivity that its disclosure must be limited to only those individuals with an absolute need to acquire the data. One method of restricting access to especially sensitive information is to permit its dissemination only within special, restricted channels of communication called Special Category (SPECAT) channels. The defendant was on several occasions in a position to have access to SPECAT communications and had the ability to transfer the information to the Soviet Union.

Some examples of operations that are planned and executed through SPECAT channels are:

a. Covert Military Operations: Disclosure of communications concerning covert operations jeopardizes the United States' ability to conduct missions vital to the national defense and world peace. The risks involve not only extreme embarrassment to our government, but also danger to the lives of the personnel involved.

b. Counterintelligence Operations: Only through the aggressive pursuit of counterintelligence initiatives such as double-agent operations, surveillance, and eavesdropping can the United States protect itself from the threat of espionage conducted against our defense establishment. Disclosure of SPECAT communications concerning such operations allows hostile intelligence services to develop countermeasures and techniques to render these operations ineffective.

c. Human Intelligence (HUMINT) Operations: HUMINT is unquestionably the most fragile of intelligence sources, due to the difficulties in recruiting human agents, the ease with which they are lost, the personal danger often involved and because the quality of information is entirely dependent on the abilities of the individual recruited. Disclosure of any information relating to HUMINT operations, even the intelligence report derived from HUMINT can lead to loss of the source, personal harm to the agent and the insertion of false and misleading information through the agent once the target organization becomes aware.

10. Based upon an analysis of Whitworth's access to classified information during his participation in the espionage scheme, on the trial testimony, and on debriefings conducted by the Office of Naval Intelligence, we wish to point out certain areas of concern:

a. Mr. Whitworth met with John Walker two to four times per year between 1976 and 1985, and supplied Walker with between twenty-five and fifty rolls of Minox film at each meeting. Since the rolls were undeveloped, Walker cannot assure us of their content, but he believes that it was largely photographed key material. The amount of money paid by the Soviets corroborates that belief. Whitworth was originally paid $2,000 per month for the material he supplied, however, this was subsequently increased to $4,000 and then $6,000 per month later in the conspiracy.

b. We also know that Whitworth compromised detailed plans for primary, secondary and emergency communications circuits which are used by the National Command Authority to maintain contact with operational units. With this knowledge, an adversary can gain significant advantage during crisis events or hostilities.

c. Whitworth also compromised operational military plans, operations orders, and operational message traffic over a significant period of time. For example, he provided the Soviets with a full year of operational message traffic from the USS Enterprise, including TOP SECRET information. He also compromised the operations order for Fleet Exercise 83-1, a unique exercise conducted near the Soviet coast by three carrier battle groups. We believe that he also compromised the communications plan for all U.S. naval forces in the Indian Ocean and all littoral nations.

11. Most importantly, the activities of Jerry Whitworth, continuing as the principal agent of collection for John Walker, permitted the Soviets to gauge the true capabilities and vulnerabilities of the U.S. Navy. The U.S. Navy is a technology-intensive service, conducting sophisticated and often sensitive operations using highly advanced warfare capabilities. Soviet access to those operations and capabilities provided them with the motivation to dramatically improve the Soviet military posture, and identified the specific steps which could achieve the largest gains relative to the U.S. It allowed them the focussed insights required to reduce their own vulnerabilities while simultaneously increasing the vulnerability of the U.S. We have seen clear signals of dramatic Soviet gains in all naval warfare areas, which must now be interpreted in light of the Walker-Whitworth espionage conspiracy conducted over approximately two decades. Mr. Whitworth's role was all the more important because of the new directions taken by the U.S. Navy during his years of collection for the Soviets. For example, through Whitworth the Soviets were able to monitor the U.S. Navy transition to use of satellite systems as its principal communication network.

12. In conclusion, the U.S. Navy and the nation have been seriously wounded by Jerry Whitworth's breach of faith and honor wherein he agreed to sell the secrets with which he was entrusted to a foreign power for personal gain. His misuse of a position of trust in naval communications has jeoparized the backbone of this

country's national defense. Recovery from the Walker-Whitworth espionage will take years and millions of taxpayer dollars. Even given these expenditures, we will likely never know the true extent to which our capabilities have been impaired by the traitorous and infamous acts of Jerry Whitworth.

WILLIAM O. STUDEMAN,
Rear Admiral, United States Navy.

Subscribed and sworn to before me this 25th day of August 1986.

PATRICK A. GENZLER,
Lieutenant Commander,
Judge Advocate General's Corps, United States Navy.

Notary service provided in accordance with 10 U.S.C. sec. 936.

UNITED STATES DISTRICT COURT, NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, PLAINTIFF,

v.

JERRY ALFRED WHITWORTH, DEFENDANT

CR. No. 85-0552 JP

I, John L. Martin, declare under penalty of perjury that the following is true and correct:

1. I am Chief of the Internal Security Section of the Criminal Division of the United States Department of Justice in Washington, D.C. As such, I am responsible for the supervision of all investigations and prosecutions of violations of the espionage law. In the performance of my official duties, I am routinely briefed on foreign counterintelligence matters by the agencies of the United States intelligence community including the Federal Bureau of Investigation, Central Intelligence Agency and National Security Agency.

2. By virtue of my position in the Department of Justice, I am aware of the facts surrounding the defection to the United States in July, 1985, of Admiral Vitaly Yurchenko, then a high official of the primary Soviet intelligence agency, the K.G.B. (Committee for State Security). The information set forth in this declaration was provided to me by United States government officials who were responsible for debriefing Admiral Yurchenko.

3. Vitaly Yurchenko defected to the United States by voluntarily walking into the United States Embassy in Rome, Italy, in July, 1985. Yurchenko was at that time a 25-year veteran of the K.G.B., having attained a military rank in the Soviet Navy of Admiral and serving since March of 1985 until his defection as Deputy Chief of the First Department of the First Chief Directorate. The First Chief Directorate of the K.G.B. is responsible for the clandestine acquisition of intelligence outside the Soviet Union, and the First Department of that Directorate is responsible for such activities in the United States and Canada. Previously, Yurchenko served as Chief of the Fifth Department of Directorate K of the K.G.B., where he supervised internal security matters, including cases involving suspected espionage by K.G.B. officers. Yurchenko had various responsibilities for internal security matters for a ten year

period, including a five-year assignment from 1975 through 1980 as principal security officer at the Soviet Embassy in Washington, D.C. In that position, he was in charge of liaison between the embassy and United States law enforcement officials concerning the security of the embassy, and had responsibility for assuring the loyalty and security of K.G.B. officers asigned to the Embassy. During his career, Yurchenko was the recipient of many awards and decorations. In July, 1985, shortly before his defection, Yurchenko received the K.G.B.'s highest honor, the title of "Distinguished Officer of the Organs of State Security."

4. One of Yurchenko's responsibilities as a Deputy Chief of the First Department of the First Chief Directorate was to review and supervise the handling of important cases in the United States and Canada. Moreover, because of his previous experience and expertise in matters of security in the K.G.B., Yurchenko was frequently consulted when K.G.B. officers came under suspicion of having been compromised.

5. As the evidence in the trial of this case showed, John Anthony Walker, Jr. was observed making a "drop" of classified information to a Soviet intelligence officer on May 19, 1985. He was promptly arrested and charged. Publicity concerning his arrest was widespread. It was also widely publicized that Walker's former wife, Barbara Walker, had tipped the FBI to Walker's espionage months before his arrest.

6. Soon after Walker's arrest and the attendant publicity, Yurchenko was briefed and consulted about the Walker case. The K.G.B. did not believe that the FBI had been tipped by Barbara Walker and suspected that one of the K.G.B. officers directly involved with Walker had been compromised by Western intelligence agencies. Because of his expertise in internal security matters, Yurchenko's advice was sought with regard to the appropriate course of action for dealing with the suspected compromise. In his position in the First Department, it was also appropriate to brief him concerning the Walker/Whitworth case. Because of the high degree of compartmentalized protection given to a case like Walker-Whitworth, Yurchenko, despite his previous assignments involving internal security and at the Soviet's United States Embassy, had not previously been aware of the Walker/Whitworth operation.

7. From his briefings, Yurchenko learned that the K.G.B. regarded the Walker/Whitworth operation to be the most important operation in the K.G.B.'s history.

8. Yurchenko stated that the information delivered by Walker enabled the K.G.B. to deciper over one million messages. Early on, operation was transferred to Department Sixteen of the K.G.B, which handles only the most sensitive and important clandestine K.G.B. operations around the world.

9. The K.G.B. officers who handled the operation received important promotions and decorations for their successes. One of these officers secretly received the "Hero of the Soviet Union" award after the Soviet Navy expressed its delight over the success of the operation. Two other K.G.B. officers involved with the Walker/Whitworth operation were awarded the coveted "Order of the Red Banner." Certain K.G.B. officers from Department Sixteen were, at various times, assigned to the Soviet Embassy in Washington solely

to handle "drops" made in connection with Walker/Whitworth espionage. The most recent of these, Aleksey Tkachenko, was returned to the Soviet Union when Walker was arrested.

10. Yurchenko was informed by a high K.G.B. official that the information learned from the Walker/Whitworth operation would have been "devastating" to the United States in time of war.

Dated: August 26, 1986.

JOHN L. MARTIN,
Chief, Internal Security Section, Criminal Division.

APPENDIX B

[From the Defense Security Institute Security Awareness Bulletin, August 1984]

PARTNERS IN ESPIONAGE

THE CASE OF JAMES HARPER AND RUBY LOUISE SCHULER

An American named "Jimmo" sporting an Irish Brotherhood medallion meets a Polish intelligence agent called "Jacques" at the Museum of Anthropology in Mexico City—such is the international, and distinctly bizarre, flavor of the latest espionage case to hit the Defense Industrial Security Program.

This is the case of James Durward Harper who was sentenced to life in prison, with a recommendation that he never be paroled, on May 14, 1984. He had pleaded guilty in April to selling classified documents to the Polish Intelligence Service. The material, classified up to Secret, pertained to survivability of the Minuteman missile system and to U.S. defenses against attack by ballistic missiles.

Harper was a self-employed electronics engineer in Mountain View, California. He first became involved with the Poles in 1975 when a business associate, William Bell Hugle, introduced him to Polish agents seeking U.S. electronics technology.

Harper was at that time running a small firm, which made and marketed the world's first digital stopwatches. He sold technologi-

cal information to the Poles for several thousand dollars. During this period, Harper did not hold a security clearance and had no direct access to classified information.

But in May 1979 Harper began what appears to have been a sort of "business-romance" with a woman named Ruby Louise Schuler. She held a Secret clearance as executive secretary to the president of Systems Control Inc., (SCI) in Palo Alto, California, a Defense contractor doing research for the U.S. Army Ballistic Missile Defense Advance Technology Center, Huntsville, Alabama. Schuler agreed to provide documents to be copied and sold. Harper contacted Hugle who, in return for a share of the proceeds, arranged a meeting with Polish Intelligence in Warsaw.

Harper conducted a total of a dozen meetings with Polish agents in Warsaw, Vienna and various locations in Mexico betwen July 1979 and November 1981. He received approximately $250,000 for documents whose loss has been rated by Army experts as "beyond calculation."

Harper and Schuler were married in October 1980. She died in June 1983 from complications of cirrhosis of the liver.

James Harper was ultimately arrested in October 1983, partly on the basis of information from a source within the Polish Intelligence Service. But his apprehension was also partly due to his own futile efforts to negotiate immunity and and a double-agent role for himself through anonymous contacts with the CIA and the FBI. Shortly after his arrest numerous classified documents were recovered from a safe deposit box in his name in a bank in Tijuana, Mexico.

The case against Harper has now been completed with his sentencing and incarceration. But certain aspects of this investigation remain active. Some details have not yet been released, and of course some never will be.

This account is based primarily upon court papers pertaining to the prosecution of Harper, especially affidavits and testimony by the FBI investigators. We have also drawn upon a follow-on inspection of the cleared facility by the Defense Investigative Service.

The most detailed account of Harper's activities was provided by prosecution testimony at a pre-sentencing hearing on April 16, 1984. This hearing did not receive extensive coverage in the press, although more limited information available at the time of Harper's arrest last October was widely reported.

As additional information becomes available on the case, we will provide follow-up articles in future *Bulletin* issues.

HIGH STAKES HAGGLING

Accompanied by his friend Mr. Hugle, James Harper sat down on July 17, 1979 in Warsaw across the table from Zdzislaw Przychodzien, known publicly as an official of Polish Ministry of Machine Industry but in fact a lieutenant colonel in the Polish Intelligence Service and head of an intelligence section or "Wydzial" using the Ministry as cover for collection operations against the West. Przychodzien was fluent in English, having been assigned to the U.S. in the 1970's with the Polish Commercial Office in New York.

Harper described the materials now accessible to him through Louise Schuler at Systems Control, including classified documents pertaining to U.S. strategic forces and ballistic missile defenses. And he provided reproduced excerpts of ten documents. (Enroute to Warsaw he had placed copies of the full documents in a safe deposit box at the Citibank in Paris.)

Przychodzien was very interested in the material. He promised generous payment, although he demurred at the American's initial asking price of one million dollars. Also discussed at this July meeting were other materials available to Harper including computer database tapes obtainable through his contacts in Silicon Valley.

Harper and Hugle agreed to meet with Przychodzien again in Vienna the following October. On that occasion Harper delivered full copies of the ten documents which Przychodzien had previewed earlier. He also provided excerpts of additional documents.

But a disagreement arose, or rather erupted, over the matter of payment. Harper and Hugle had come down a good deal from their original demands, but they understood that $15,000 would be paid for one of the ten documents. When Przychodzien declined to pay that much Hugle started a shouting match which quickly broke up the get-together, which was taking place in a public lounge at the Hotel International.

Harper had travelled to Vienna with Louise Schuler. They left the city immediately following this incident and returned to California. Harper was naturally unsure of his position with Przychodzien.

It appeared that the Poles were not as interested in the classified Defense documents from SCI as he had originally thought, so he buried them, in an out-of-the-way location in the San Joaquin River delta near Stockton, California—just for safe-keeping in case a buyer could later be found.

SOGGY SECRETS AND GREETINGS FROM YURI

At this point Harper wanted nothing further to do with the excitable Mr. Hugle, but he was able to reestablish contact with Przychodzien through a friend in Switzerland, and he returned to Warsaw in May 1980 with the Silicon Valley database tapes and without any classified documents.

But it was the classified ballistic missile material that Przychodzien really wanted. The intelligence officer paid $10,000 for the ten documents delivered at the stormy meeting in Vienna, apologized for the misunderstanding and urged Harper to come back with all of the Defense documents he could get his hands on.

So Harper went back to the delta, dug up his "stash" and transported the additional documents to Warsaw (via Vienna and Geneva) the following month (June 1980). Harper later estimated that this second delivery of reports, some of which were classified, weighed about 100 pounds. The documents were somewhat the worse for their seven month interment on the banks of the San Joaquin River. But Przychodzien's people worked through the night of June 5 to separate the matted pages and restore the materials to decipherable condition.

On June 6 the documents were brought to the Soviet Embassy where a team of 20 KGB experts, flown in specially from Moscow, declared them to be genuine and extremely valuable. Harper was paid $100,000 on this occasion. A month later Przychodzien and his unit received a commendation for their efforts, directly from KGB Chairman Yuri Andropov.

JIMMO MEETS JACQUES

Harper next returned to Warsaw in September 1980, this time bringing along a document registered for the safe in his wife's office, i.e., an inventory of all documents in the SCI president's security container. The Poles selected several items for purchase and Harper delivered them during visits to Warsaw in October and November 1980, receiving $20,000 in payment.

During the November meeting with Przychodzien Harper was instructed to meet next time in Mexico City with a Polish agent whom he knew only as "Jacques." Harper himself was given the code name "Jimmo." He occasionally wore an "Irish Brotherhood" medallion, and this was to be used as a recognition device. In addition, Harper wrote a limerick on the back of the laundry slip. This was then torn in half, and Jimmo and Jacques were to confirm identities by matching the halves of the paper.

The first meeting with Jacques took place as agreed at the cashier cage of the Museum of Anthropology on December 14, 1980. Harper brought no documents, treating the occasion as a dry run to establish contact and "get the feel of the city." Jacques paid him $10,000 anyway, and at the next encounter in the same city two months later Harper brought nine Secret documents and received $60,000.

Following one more transaction with Jacques (eight classified documents and excerpts of 30 more, in return for $50,000), Harper told the agent in September 1981 that he was dissatisfied with the payments he was receiving. He brought no documents to the September meeting, in Guadalajara, and received no payment, although Jacques had brought along $30,000 for the 30 documents previewed last time in extract. It was agreed that Harper would go back to Warsaw to work out his complaints with Przychodzien directly.

This was in fact the end of Harper's active dealings with the Poles. He made a trip to Warsaw in November 1981 and spoke with Przychodzien, but he remained dissatisfied with the payments offered and no further contacts ensued.

Before going to Warsaw Harper had driven with Louise to Tijuana and placed his remaining collection of classified documents in a safe deposit box, where they remained until retrieved by the FBI, with Harper's cooperation, following his arrest.

These were actully the last documents available to Harper, since Louise lost her clearance in August 1981—not due to any suspicion of her activities but rather due to acquisition of her company by a foreign firm.

Under an arrangement approved by the Department of Defense, SCI's Defense contracts have been retained by a "spin-off" company insulated from the parent by a stock proxy agreement. The fa-

cility clearance for this subsidiary was later upgraded from Secret to Top Secret. But Ruby Schuler remained an employee for the original SCI organization, now under British ownership, and her Secret clearance was administratively terminated as a result.

She had major surgery in August 1982 and died the following June of cirrhosis of the liver. Her death certificate lists "alcoholism" as a "secondary cause" of death.

PLAYING BOTH ENDS

In September 1981, at the time he was becoming increasingly unhappy about his exchanges with the Poles, Harper contacted attorney William Dougherty requesting that Dougherty act as go-between in negotiations with the CIA and FBI. Harper wanted to arrange immunity from prosecution in exchange for information on his activities and services as a double agent. While concealing his identity from the lawyer, he provided detailed written and tape-recorded accounts of his espionage activities through Dougherty to the government. This continued for two years until Harper's ultimate arrest, although the government showed no willingness to agree to his terms.

Investigators succeeded in positively identifying him in March 1983. He was immediately placed under physical surveillance at his home in Mountain View, California, where he was at that time living with Louise. Wiretaps were also authorized and installed on their telephone.

Investigators were able to learn the location of a storage locker where Harper kept records of his activities. They also learned that he was planning overseas travel and was again in contact with the Swiss friend who had arranged earlier meetings with Przychodzien.

He was arrested on October 15, 1983, forestalling any chance that he would turn over his remaining documents.

THE KGB CONNECTION

One lesson of this case is unmistakable confirmation of the intimate ties between Warsaw Pact intelligence services and the Soviet KGB. It is clear not only that the Polish Intelligence Service works closely with the KGB, but that they in fact work for the KGB.

When Harper brought his main installment of documents to Warsaw in June 1980 the Poles spent the night putting the pages in order, but once collated the materials were immediately turned over to the Soviets for evaluation and analysis.

Harper has stated to the FBI that the tasking presented him by the Polish agents was derived from a "master shopping list" provided by the Soviets. And this has been confirmed by the Polish intelligence officer who served as a source in breaking the Harper case. U.S. investigators have not revealed the source's identity but they have testified that he was an officer of the Polish Intelligence Service at the time Harper was active, that he was a close colleague of Zdzislaw Przychodzien and that he served as liaison officer with the KGB for Przychodzien's intelligence unit. The source has confirmed that Polish agents respond directly to detailed tasking from the KGB, with military collection as a top priority.

The Polish source was aware of Harper's activities, although he did not know Harper's identity. Przychodzien had told him of the initial meetings with an American, fitting Harper's description, who had access to ballistic missile information.

He even recalled seeing a phone message from Hugle written on Przychodzien's desk calendar at the time of those first meetings in October 1979. This inside information confirmed the authenticity of Harper's accounts once his anonoymous statements began coming in.

SECURITY IN THE FACILITY

Information so far available does not reveal any major security deficiencies at SCI which can be identified as contributing directly to Harper's and Schuler's activities. She apparently removed the documents from the facility to be reproduced at home on a paper copier which Harper had bought for the purpose. As in most facilities, governmental or industrial, there were no searches at the exists to prevent removal of classified material.

Schuler was noted in the facility during evenings and weekends. On at least one occasion Harper was with her. But this was not a violation since he was escorted—by Schuler! Unexplained off-hours activity has often been highlighted as a possible indication of espionage, and this is another case in point.

As a result of the case the company has centralized its classified document storage at one location under direct control of the security officer (something which would obviously not be possible for a larger facility), and they have implemented tighter personnel access controls for non-working hours.

There are some indicators that certain adverse information regarding Louise Schuler was known to co-workers and company officials and was not reported. She was, first of all, an alcoholic and ultimately died of complications from that disorder. Quotations in the press indicate that co-workers were aware that she carried vodka in her purse and drank on the job. An inquiry into that issue might have revealed some indication of her illicit activities, or possibly exerted some deterrent effect.

In addition, a former employee of the company, also a cleared individual, had a close involvement with Louise during much of the period in question, and he was aware not only of her drinking but also of her unexplained income. She does not seem to have flaunted her ill-gotten gains in a public sort of way, and most co-workers would have had no occasion to notice anything out of the ordinary.

But this other employee was with her on at least one occasion when she placed a large stack of $100 bills in a safe deposit box at a local bank, and he did not report this.

THIS CRIME DIDN'T PAY

Much of what makes the Harper case an interesting story also makes it an atypical story, therefore limiting its value as a source of "lessons-learned" for future reference and edification. But it does bring to the public view a rare glimpse of the inner workings of a foreign intelligence service. And it emphasizes the clear and present danger which espionage poses to our national security.

The case dramatically demonstrates that our security system is inherently and perhaps inevitably vulnerable to betrayal from within. Procedures and physical barriers can keep uncleared people from direct access to classified material. But when a cleared person goes bad, our defenses have already been breached and some damage is bound to occur.

Above all, the case highlights yet again that our system rests ultimately upon the integrity of the cleared individual. We must strive to indentify and motivate that quality, however elusive.

Finally, the sentence received by Harper provides a "lesson-learned" that is hard to overlook.

At the time of sentencing Judge Samuel Conti emphasized that he had "never heard the defendant say that he was sorry," and he called Harper's criminal activities "beyond comprehension or toleration." "Your actions have exposed all of our people to risk and danger," he said, "a danger that could well extend into the 21st century."

"There can be no crime more serious than that of selling our country's defense secrets to a foreign government," the Judge stated. "Your crime concerns each and every living and yet unborn citizen of this country," and it threatens "the very heart and existence of our freedom."

"It is ironic, indeed, that you pled guilty on April 15th, and that's the very day that all federal income taxes were due. It goes without saying that a great portion of the billions paid in taxes goes for national defense and yet you, for your own personal greed, would cause many of these billions to go for naught and to the advantage of a foreign power."

The judge then imposed the maximum sentence—life imprisonment, with recommendation against parole.

APPENDIX C

[From the Defense Security Institute Security Awareness Bulletin, June 1983]

CAUGHT UNAWARES: THE CASE OF WILLIAM BELL AND MARIAN ZACHARSKI

Marian Zacharski arrived in Los Angeles from Poland in late 1976. He was assigned as West Coast Branch Manager for the Polish American Machinery Company (POLAMCO), a U.S.-incorporated firm serving as marketing arm for the Polish trade agency, Metal Export.

But machinery was not Zacharski's only business. He was also covertly assigned by the Polish Intelligence Service to spot and recruit agents within California aerospace industry. And he was for a time highly successful in both his occupations. By early 1981 (at the age of 29) he had been appointed president of POLAMCO, and he had recruited at least one agent with access to important classified weapons information and technology.

Thereafter, Zacharski's fortunes took a turn for the worse, and by the end of 1981 he was serving a life sentence for espionage against the United States—but not before doing both a lot of good for Polish exports and a lot of harm to U.S. national security.

William Bell was Zacharski's agent. He was born in Seattle, Washington on May 14, 1920. He was employed an an engineer with Hughes Aircraft Company and met the Polish businessman in 1977 at the Cross Creek Apartments in Playa del Rey where both were residents. The two shared an interest in tennis as well as a common concern with the aerospace industry, where Zacharski sold much of his industrial equipment.

After almost a year of purely social and recreational contacts, Zacharski began to ask Bell for unclassified literature from work. Then he asked for "interesting" material and received first Confidential, then Secret documents to look over. He paid Bell lavishly for his minimal "consulting" work. And when Zacharski proposed that Bell, for additional thousands of dollars, photograph classified documents and carry them to Europe to meet other Polish representatives, Bell was ready to go along. Soon he felt "over his head" and too committed to back out. William Bell is now in prison, serving an eight-year sentence.

Zacharski's recruitment approach was a standard one. It should be as familiar and hence as ineffective as attempts to sell shares in the Brooklyn Bridge. But Bell's susceptibility was not the result of tender years, or slim experience or lack of education, training or intelligence. He was 57 years old when he meet Zacharski, with 25 years in Defense work, a B.S. in applied physics from UCLA and two overseas tours with his company.

Bell had been briefed on the threat of hostile intelligence services, but he did not recognize the classic approach when he encountered it in real life. He did not believe that it could actually be happening to him, that this amiable Polish tennis buff (who reminded him of his estranged older son) could possibly be anything other than what he appeared to be.

Bell was experienced, educated and informed—but not *aware*. We are using his story, as he has recommended that it be used, to enhance the awareness of others who may face a similar approach—and in the hope that they will respond by promptly reporting such contacts to security officials, for their own protection and for the protection of U.S. national security.

I. THE FACTS

Marian Zacharski was arrested for espionage in June 1981 and went to trial in October. He was convicted largely on the basis of William Bell's testimony against him, and Bell's lighter sentence was based in part upon consideration of his cooperation with the government in the final stages of the investigation and the trial. This account of the Bell/Zacharski espionage case is based primarily upon the transcript of Zacharski's trial. It also draws upon Bell's testimony in May 1982 before the Senate Permanent Subcommittee on Investigations.

Troubled times

In the Fall of 1977, when he was first introduced to Marian Zacharski at the swimming pool of the Cross Creek Apartments, William Bell had recently returned to Los Angeles from an assignment in Brussels as Manager of European Operations for the Radar Systems Group, Hughes International Corporation. He was now a Project Manager in the Advanced Systems Division, Radar Systems Group at the main Hughes facility in Los Angeles.

Bell held a Secret security clearance and was responsible, as he later testified, for "development and promotion of the radar fire control product line for tank vehicles." He had been with Hughes since graduation from UCLA in 1952, employed entirely at the Los Angeles facility except for two European assignments (in the mid-1960's and from 1974 to 1976).

In his Senate testimony Bell stated that these overseas assignments had been "financial nightmares" for him, "although they are touted as glamorous and lucrative." Upon his return in 1976, he recalled, he was "pursued by four separate IRS offices for back taxes on disallowed deductions primarily arising out of my overseas assignments." The year of 1976 was in fact a low point in Bell's life for a number of reasons. He was divorced from his wife after 29 years of marriage ("in an extended proceeding") and was faced with alimony payments of $200 per week. His accumulated debts forced him to file bankruptcy in July 1976. During the previous year, Bell's family had suffered a tragic loss when his 19-year-old son died in a camping accident in Mexico.

In addition to finanical hardship, divorce and personal tragedy, Bell also later recalled feeling "like an outsider" upon his return to the Los Angeles plant. "I returned from Europe to find a younger

group at Hughes and I [was] shunted off to a quiet back room." But regardless of any disappointment with his assignment, Bell was in fact given major responsibilities for development of advanced weapons systems—a fact which Marian Zacharski was quick to learn.

New beginnings

When he met Zacharski in 1977 Bell was attempting to make a new start. He had remarried ("to a young Belgian citizen," formerly his secretary overseas) and had taken up residence with her and her six-year old son at the Cross Creek Apartments. He was making a gradual financial recovery (although alimony, taxes and debts still put a strain on his $35,000 income). And he found comfort in the companionship of a close friend:

> Zacharski and his wife moved into the apartment complex and I began to play tennis [with him] on a daily basis. He slowly became my best friend. He was about the age of my oldest son who had been close to his mother and quite distant from me since our divorce.

Marian "made friends easily," Bell recalled. The two couples socialized frequently both by themselves and with an informal "little United Nations," a social group at the complex consisting of couples one or both of whom were foreign nationals. And the two men found common professional interests as well. Zacharski was a skilled and successful salesman of industrial equipment and the California aerospace industry was one of his principal sales targets. He naturally discussed the aerospace business with his tennis partner and, in about mid-1978, he asked Bell for help in making contacts at Hughes and other companies in the field.

Bell gave Zacharski's name to a purchasing manager at Hughes and also contacted people at Lockheed and Northrop. And for this Zacharski paid him approximately $5,000. At the trial, the cross-examining attorney wondered why Bell had not been suspicious of such generosity. He had been, he claimed, though evidently only temporarily. "To recieve four or five thousand dollars for doing pratically nothing made me very suspicious."

> Q: It also made you very glad, did it not, Mr. Bell?
> A: It sure did. I needed the money.

The conscientious consultant

Bell and Zacharski discussed the possibility that Bell might be permanently retained by POLAMCO as a "consulting engineer" and sales advisor, although the terms of the arrangement were left studiously indefinite ("I was working, in a way, and talked about working as a consultant for POLAMCO . . ."). Bell began, again around mid-1978, to provide printed material from the office, to help Zacharski keep abreast of sales opportunities. "It started out [with] simple things," Bell later told the Grand Jury, "like the Hughes News," the company newspaper.

Then came documents of more technical substance. He brought Zacharski copies of the Hughes "Vector," a technically-oriented publicity sheet on company programs. Zacharski had specifically requested these openly-published materials. But then Bell began to

volunteer materials in response to Zacharski's general expressions of interest. "I could tell from our conversations that they were things that he would like to see." "We would be talking about it at the tennis court—unclassified documents in the beginning."

During the summer of 1978 he provided Marian with several documents "related to items that were machined."' These were unclassified, at least for the most part, but "there was possibly one confidential. . . . I'm not certain." Bell has never been sure of exactly when he first showed Zacharski a Confidential document—or just which or how many such documents he had compromised.

He may also have been uncertain in his grasp of security requirements for the handling of Confidential material, as indicated by this courtroom exchange between Bell and prosecutor Robert Brewer:

> Q: Would that [taking documents home] be a violation of . . . security policy?
>
> A: Not a confidential document no. You can bring confidential documents home. You cannot bring secret documents home.

CAWGS, LPIR and DPWS

The Secret documents which Bell compromised can be more reliably identified since the company maintained accountability records for them (not required by the *Industrial Security Manual* for Confidential). Bell determined that his first transfer of Secret material occured in October or November of 1978 when he lent Zacharski (at the tennis court) Copy No. 8 of the "Proposal for a Covert All-Weather Gun System, Executive Summary, Volume I." Bell was the author of this material. He wanted Zacharski to understand his role at Hughes and he wanted to impress him with his work. "I was proud of it," he said of the Executive Summary, "and I gave it to him." Later Bell turned over an unclassified document on the same subject and stamped it Secret "to make it look more important."

The Covert All-Weather Gun System ("CAWGS") was the primary development project under Bell's technical management at that time. It envisioned the application to tanks of the Low Probability of Intercept Radar ("LPIR") or "quiet radar." LPIR utilizes a disguised radar signal which is difficult for enemy targets to identify as radar; they are thus prevented from taking evasive action or using the radar signal for directing return fire. The CAWGS, subsequently redesignated the Dual Purpose Weapon System or "DPWS" (to be used against both aircraft and other tanks), was Bell's main responsibility throughout his relationship with Zacharski. It was, according to trial testimony, the principal program compromised by his espionage activities.

A Friend in Need

It was announced in mid-1978 that the Cross Creek Apartments would be converted to condominiums. Bell and his wife wanted to remain, but he was worried that he could not make the down payment required to purchase this unit. His friend Zacharski said he might be able to help. And in February 1979 he provided Bell with

$12,000 in two payments handed over in envelopes at the door of Bell's apartment. They were speedy and uncomplicated transactions, as Bell later testified: "Q: Did you say anything to him? A: 'Thanks.' "

He used the money for the condominium payment and for back taxes. He assumed that the money was from POLAMCO's "marketing" fund. And he credited Marian's good will with inspiring this generosity. "I thought we were good friends and I knew he would like me to stay in the apartment complex. I wanted the condominium and I accepted the money."

Foreign liaison

Bell still thought it was in connection with "consulting" activities when Zacharski suggested, in the Summer of 1979, that he travel to Europe to meet certain unidentified Polish representatives ("whom I thought would be POLAMCO people"). He was asked to photograph documents from work and bring the film with him to the meeting in Innsbruck, Austria. Marian had earlier given Bell a Canon movie camera, which turned out to have a frame-by-frame capability ideal for photographing documents. He provided a tripod and special film and instructed Bell in using the camera in his bedroom.

William Bell departed on the first of four overseas "missions" on November 26, 1979. Marian gave him about $2,500 for expenses, although Bell's wife was an airline flight attendant and his trans-Atlantic fare was $18. On the morning of November 30 he went to a pre-designated restaurant in Innsbruck and was met by a man who introduced himself as "Paul" and asked "are you a friend of Marian's?"—the agreed-upon recognition signal. The two left the restaurant and entered a car driven by another man (name not recalled) and drove to the outskirts of Innsbruck.

Bell handed over his film and the three men discussed Bell's work, the types of information he should attempt to collect and the need for secrecy and security. At one point Bell was shown a picture of his wife and son. "He [Paul] told me that I had a lovely family. Then he said that our security depended upon each other and that if anybody got out of line that he'd take care of them." The Poles did not dwell on the point, but Bell clearly perceived an "implied threat" in Paul's words. Before leaving Innsbruck, he received $7,000 and agreed to another meeting in the same city in May 1980.

Lost innocence

When he returned to Los Angeles, Bell received an additional list of desired collection targets from Zacharski. On this and other occasions he was surprised at Zacharski's highly specific knowledge of system designations and even particular document numbers.

> Q: And did you ever ask Mr. Zacharski where he obtained those numbers:
> A: Yes.
> Q: What did he say, if anything?
> A: He didn't answer me. He just smiled.

By now, at the end of 1979, Bell could no longer maintain the illusion that he was involved in a (more or less) innocent consulting arrangement with POLAMCO. It was clear, as he testified, that he was "conducting espionage" for "agents or officers of the Polish Intelligence Service." And Zacharski himself dropped any such pretense after that time. He made no more requests for assistance in promoting machine tools.

Bell took three more trips to Europe, meeting with one or both of the Polish operatives at Innsbruck in May 1980, at Linz (Austria) in October 1980 and at Geneva in April 1981. Prior to each meeting he photographed several documents with the movie camera in his apartment (when his wife was away). At the Innsbruck meetings he provided film of unclassified and Confidential documents. At Linz and Geneva he turned over copies of Secret material related to the DPWS and LPIR system. He continued to receive substantial payments, in bills and in gold, from both Zacharski and the handlers overseas.

Deja Vu

After Geneva, Bell's next meeting with the Poles was to be in Mexico City. He was uneasy about transacting his business there, he testified, in part because "Mexico City is where a spy was caught, I don't recall his name." The name, of course, was Daulton Lee, accomplice of TRW spy Christopher Boyce. But Bell was relieved of the necessity of following Lee's footsteps to Mexico. He was called to Hughes security on June 23, 1981 to be questioned by the FBI. At the trial Special Agent James Reid recalled the crucial point of the interrogation as follows:

> [Reid]: I showed Mr. Bell a translation of a Polish newspaper article which indicated an individual who had been assigned to the U.N. In New York had defected to the United States Government. I then explained to Mr. Bell that this individual had in fact defected, and that he had been providing the FBI with information concerning activities of the Polish Intelligence Service in this country.
>
> Q: What if anything did Mr. Bell say?
>
> A: Mr. Bell asked, "Did he mention me?" And then without waiting for an answer, he said, "this is very serious. I would like to talk to an attorney."
>
> [Reid told Bell that he could talk with a government attorney or make a telephone call to an attorney of his own.]
>
> Q: And after you said that, what happened?
>
> A: Well, at that point Mr. Bell physically slumped in his chair and he said, "I did it. I do not need an attorney."

Bell signed a confession and agreed to cooperate in the further investigation of Zacharski. On June 28 he was fitted with a hidden recording device when he met with Marian on the apartment grounds to discuss further payments and certain sensitive programs at Hughes which Zacharski was interested in targeting. Zacharski was arrested shortly thereafter.

II. THE LESSONS

The Bell case, like any other espionage case, has its unique and peculiar elements. But it is, by and large, a "text-book" case which confirms many of the long-standing precepts of counterintelligence, as well as patterns derived from recent espionage cases.

Motive and predisposition

Financial gain was Bell's primary motivation. This is typical of most recent cases, and his testimony was quite clear on the point. Politics or ideology did not play a part:

> Q: You are not, in other words, a secret Polish patriot?
> A: No I am not.

The motivation was primarily mercenary. "Mr. Zacharski had found a fool that needed money. I had a weak spot. He took advantage of me." Bell also cited the veiled threats from "Paul." This played some part in his thinking and discouraged him from pulling out once he was involved, but "the motive was always money." ("Q: Was it worth it? A: No, absolutely not.")

Financial difficulties and other personal problems were an important cause of Bell's susceptibility to recruitment. From his trial testimony, it appears that Bell faced the kind of difficulties which everyone encounters at some time during life, although the coincidence of several misfortunes in quick succession clearly contributed to an imbalance in judgment. Withdrawal of clearances in cases like this would generally be both cruel and unuseful. But certainly whatever positive assistance or counselling an organization might provide to employees in trouble, combined with an active program of defensive security training, will help to ensure that a person like Bell is not so choice a target for a person like Zacharski.

Job dissatisfaction or some element of grudge against the company or the U.S government have figured as predisposing elements in several recent cases (Boyce, Kampiles, Edwin Moore, etc.). Bell's remarks display some signs of disgruntlement with Hughes. The European assignments were not as "glamous and lucrative" as they were "touted" to be; he felt like an "outsider" among the younger personnel at the Los Angeles plant—and so forth. But here again Bell's difficulties were of a rather ordinary sort, providing no obvious warning of an employee who was ready to take desperate measures.

Espionage indicators

Several attempts have been made in recent years to draw up a behavioral profile of the typical spy, to identify the patterns of activity which are characteristic of espionage in progress. A listing of such "warning signals" published recently by the U.S. Air Force Office of Special Investigations (AFOSI) is provided following this article (below, p. 122). Bell's is presumably one of the cases which underlies this analysis and his activities do in fact lend credence to several of the major espionage indicators. AFOSI calls these factors an "Ounce of Prevention" since early reporting of suspicious behavior may help to halt an espionage operation before irreparable damage is done.

Unexplained affluence is well known as a possible tip-off to ongoing espionage and certainly Bell received a substantial increase in income from his illicit activities. His estimates of the total amount varied wildely, from $70,000 to $170,000. Payments specifically cited during the trial were totalled to between $101,000 and $103,000.

Bell spent or invested most of the money, although some of the gold remained unconverted at the time of his arrest and was confiscated by the government. His testimony indicates that he was relatively conservative in his use of the funds, and even the luxury items cited—a "red Cadillac," a $2,000 necklace for his wife and a brief vacation to Rio de Janeiro—would not necessarily appear extravagant for a family with an income of $52,000 (in 1980): Bell, $40,000, his wife, $12,000). Much has been made in press coverage regarding the "young stewardess" angle in the case, but there is no indication that Bell's second wife either contributed to his financial setbacks or drove him to seek new income in support of an inflated lifestyle. (And she was not in fact an airline flight attendant when she met and married him but entered training in Janaury 1979.)

Bell's windfall earnings were directed not to high living but primarily to hastening his recovery from bankruptcy. His was a case not so much of unexplained affluence as of unexpected solvency. Any major alteration in financial circumstances may be of significance when personnel with access to classified information are involved.

Attempts to gain unauthorized access to classified information (e.g., beyond legitimate need to know) are often characteristic of diligent spies, but Bell seems to have avoided this pitfall. He was apparently a cautious (or lazy) agent and did not seek out information beyond his assigned projects. The major compromises confirmed at the trial (LPIR, DPWS) fall within the scope of his primary duties as a project manager.

Removal of classified material from the facility is a more or less inevitable accompaniment to spying, and certainly Bell took some risk in this regard. When he carried documents home to be photographed he was vulnerable to detection since Hughes had a policy of random searches at the plant exits. Either Bell was lucky in his timing or he was somehow able to anticipate the searches. In any case he was never caught in the act.

Foreign travel, on a regular basis and without sufficient explanation, is another "tell-tale sign" displayed by Bell and one which evidently contributed to his detection. His trips to Europe were partially legitimized by company business and family visits. But testimony (Bell himself and by a Hughes security official) indicates that his overseas travel—and, on one occasion, incomplete reporting of his itinerary—was a factor which helped to place him under suspicion.

Awareness: The best prevention

So Bell confirms, to some degree, certain of the behavioral patterns associated with previous cases of this kind. Financial difficulties and job-related dissatisfaction can predispose an individual to espionage. Unexplained income, unauthorized removal of documents and unexplained foreign travel may be indicators that espio-

nage activity is underway. But the case also confirms the difficulty of applying this sort of preventive counterintelligence to real-world situations, without the benefit of "20/20"hindsight." The real "ounce of prevention" would have involved measures to forestall Bell's recruitment in the first place. And there is good reason to think that this could have been done—with the infusion of a little more awareness.

"Who Would Expect it . . ."

This presupposes that Bell was genuinely unaware, during the initial stages, of what Zacharski was up to. A more cynical view might suppose that he knew exactly what was happening all along and complied with Zacharski's wishes, from the beginning, with his eyes wide open. But those who investigated and prosecuted Bell are inclined to accept his account of the evolution of the case. And Bell has testified that, when he returned to the state-side facility from Brussels, he assumed that his worries were over where hostile intelligence activities were concerned. "When you are sent to Europe," he told the Senate Subcommittee, "you are told to expect attempts by foreign spies, but whoever would expect it to happen here at home?

He received the required briefings and signed the required forms upon rejoining the Los Angeles organization, but apparently treated them as a matter of insignificant routine. A "Security Briefing and Termination Statement" was introduced in evidence at the trial, and he acknowledge having seen it: "I recall signing the normal form you sign when you hire into the company. . . . There are many forms you sign and I am sure that was one of them."

"Whoever would expect it to happen here at home?" It was in this innocent frame of mind that Bell initially made the acquaintance of the Polish machinery salesman and then agreed (in fact eagerly sought) to serve as a consultant for POLAMCO, an arrangement which included providing inside information on his company. The delusion persisted right up to his first overseas visit:

> Even as I went to Innsbruck, Austria, I was rationalizing and kidding myself that the persons I would meet were representatives of POLAMCO, that this was just the kind of industrial espionage that goes on all the time.

After his return from Innsbruck, Bell knew exactly what he was doing and exactly what had been done to him. Why he did not extricate himself at that point is a complex psychological question involving a confluence of material inducements, Zacharski's personal magnetism and "Paul's" implicit menace. For whatever reason, Bell now felt genuinely trapped. He told the Senators after his conviction: "There is little left of my life now but I feel I am freer in prison than I was with Zacharski."

The classic modus operandi

Clearly there was more to this entrapment than simple monetary temptation. And we must not take too literally Bell's own statement that he was "a fool that needed money." A fool he may have been and he was certainly hungry for cash. But too much

stress on Bell's foolishness can lead us to ignore Zacharski's skill. Preoccupation with financial motives, moreover, can obscure the fact that many months of cultivation *preceded* the first mention of money between Zacharski and Bell. We must not ignore the subtle but powerful psychological influences which reinforced the material incentives once offered and laid the groundwork for Bell's receptivity, by creating a willingness to regard Zacharski's offers as well-intentioned, as motivated by friendship and a good will.

Cover

Bell's recruitment was the result (not necessarily the only result) of a carefully planned and orchestrated intelligence operation. As the focal point for this operation, Zacharski was provided with the best possible cover for his activities, a cloak of propriety calculated to inspire the least possible suspicion. To begin with, his nationality was in his favor. As a citizen of an Eastern European country he would not present the same threatening image as a Soviet national—although there can be no doubt that the information he collected was to be shared with Poland's Warsaw Pact ally. (It might be recalled in this connection that during the year Zacharski arrived, 1976, a Presidential candidate had come very close to declaring Poland a member of the free world!)

In addition he was provided with a commercial rather than a diplomatic position. He was employed, in effect, by the Polish government, but as a salesman of industrial equipment he assumed an image which was less official and hence, again, less threatening. In addition, he was exempt from travel restrictions imposed upon diplomats from communist countries and had more flexibility of movement and greater access to U.S. industrial facilities and personnel. Of course commercial status carried with it a certain disadvantage: no diplomatic immunity. Zacharski is no doubt now hoping to be exchanged for someone imprisoned in the Soviet bloc, but there have been no indications that a swap is contemplated.

Once fitted with suitable camouflage, Zacharski was introduced into a promising hunting ground, the technology-rich area of Los Angeles, California. He moved into an apartment complex where many executives and engineers of aerospace companies were residents. And he set to work.

Closing in

Having met William Bell, as he must have met many others in similar professional positions, and having decided to proceed with cultivation, Zacharski worked with extreme caution and practiced subtlety. He was a skilled salesman and master persuader and well equipped for his task.

Bell testified that they first met in Autumn 1977. He could recall no requests of any kind from Zacharski until mid-1978. So Zacharski spent the better part of an entire year simply making friends with his prospect, insinuating himself into his personal life, meeting and befriending his family, assessing his character traits (and flaws), learning his likes and dislikes (and sharing them), discerning his weaknesses and above all his needs.

Only after many months of this did he *begin* seeking active assistance from Bell and overtly feeding his desire for money. Corne-

lius G. Sullivan, a former counterintelligence agent with the FBI, testified at the trial that this is a crucial "dividing line" in the process of developing an agent, the boundary between a simple social relationship and one involving overt exchange. This "barrier" is typically overcome, he said, by first requesting unclassified and seemingly innocent items—and this of course is the approach which Zacharski adopted.

There is also a second dividing line—between providing innocent, public materials and handing over restricted, sensitive and/or classified items. Zacharski used the "consulting" process to bridge the barrier between legal and illicit activities, and this was perhaps the central gambit in his very successful strategy. It was so effective in fact that Bell apparently volunteered the first transfers of classified material on his own initiative.

The "Pitch"

Offering the prospect of a consulting arrangement, as a prelude to espionage, proved successful in this case for a number of reasons. The promise of additional income appealed to Bell's financial hunger, of course. And it must also have appealed to his entirely normal professional vanity to be asked to lend his technical expertise and the benefit of his contacts in the industry. Because the arrangement was obviously improper to a degree, it introduced a surreptitious element into the Zacharski/Bell relationship and helped to ease Bell toward a fully clandestine role as a full-fledged spy. (Bell explained his additional income to his wife as coming from work for a Swiss aircraft firm. He asked her to be discreet about the arrangement, stating that Hughes would not approve of his consulting for a competitive firm.)

Perhaps above all the consulting arrangement permitted Zacharski to deceive Bell, and Bell to deceive himself, into regarding the initial compromises of national security information as a venial sort of "industrial espionage." "Within the avionics industry," Bell told the Senate Subcommittee, "it is a common practice for all companies to obtain the secrets of their competitors by the same techniques Zacharski used with me." He thought of POLAMCO as "an American company." They had offered him a job which would be "the solution to all my problems." And providing them with inside information from Hughes would only be adhering to the common practices of the industry, as he interpreted them:

> An engineer for one company is interviewed by the management of another. Considerable benefits are dangled in front of the engineer in terms of increased earnings and better position. He is asked to produce samples of his work and this is normally done without regard to security classification. . . .

Whether or not Bell accurately describes a common practice, he certainly does reflect a common attitude—"Everybody's Doing It." Zacharski exploited this attitude and used the consulting ploy to ease Bell almost imperceptibly into his intitial ventures in the illegal exchange of information. After that Bell felt that it was too late to back out, and it was indeed too late to prevent some damage to the national security, since some damage had already been done.

Thinking about espionage

"It would have been so much easier to warn me." This statement during Bell's Senate remarks does not excuse his crime—and it was not offered as exculpatory—but it may be the central lesson-learned in the case. Either he was not sufficiently warned, or he did not heed the warnings he received. Whether the blame is laid upon the system of security education or upon the individual, the damage to national security is the same. And better awareness training—drawing upon Bell's case as a cautionary example—should help to warn others similarly situated. As Bell himself put it: "Every person employed in a security job should know what I did to myself, to my loved ones and to my country and [should] realize how easy it is to get trapped."

In an article published on the anniversary of the trial, the Los Angeles *Daily News* stated the lesson of the Bell case very aptly: "When William Holden Bell worked for Hughes Corporation, he never seriously thought about espionage. But it happened anyway." Thinking seriously about espionage, about the reality of espionage, is the first requirement of security awareness. And security awareness is the key to security compliance.

III. THE BOTTOM LINE

Based upon the lesson of Bell/Zacharski, and other similar cases, awareness briefings should stress the following:

What you should know

There is potential danger in any sustained contact with a communist-country national (and not just with Soviets). You are not required to avoid all contact; just be careful.

Recruitment is a subtle, gradual process (a "long, bit-by-bit thing," Bell called it). Cultivation may last for months or years and initial active involvement may have nothing to do with espionage in any recognizable form.

Recruitment may involve no elements of blackmail or threat, so those who regard themselves as "clean-living" may nonetheless be susceptible to this sort of activity.

Positive inducements are generally more effective than threats. And such inducements will involve psychological ploys (friendship, flattery, sharing of common opinions/interests) as well as (and usually prior to) material offerings.

"Entrapment" once it comes is as much a psychological as a material entanglement, and commitment (as in Bell's case) may only be recognized after the fact.

What you should do

As a cleared contractor employee, you *must* report to the security supervisor: 1) all acts of espionage or suspected espionage, 2) any attempt to gain unauthorized access to classified information, 3) any compromise or suspected compromise of classified information, 4) plans for travel to (or through) a communist-controlled country, 5) plans to attend any professional meeting where communist-country nationals may be in attendance, 6) plans to host a facility visit by communist country nationals.

You should (for your own protection) report any contact, particularly sustained contact, with a communist-country national, even if purely personal and seemingly casual. In this way you avoid any suspicions which might arise regarding your own conduct and permit authorities to warn you if the individual is suspected of intelligence involvement.

POSSIBLE ESPIONAGE INDICATORS: "AN OUNCE OF PREVENTION"

(Source: U.S. Air Force Office of Special Investigations (AFOSI)
(Adapted from TIG Brief 18, 1982))

From an analysis of confirmed espionage cases, AFOSI has developed a listing of characteristics shared by several of the spies in varying degrees. *While no element of this list of "warning-signs" is, in itself, proof of an individual's involvement in espionage,* observation of such characteristics in the behavior of an individual with access to classified information should be a matter of concern to security and supervisory personnel. Even where espionage is not present, several of the characteristics may be indicative of problems in suitability or security which cannot be prudently ignored.

The list as presented here has been adapted to reflect the special requirements applicable to Defense contractors under the *Industrial Security Manual for Safeguarding Classified Information (ISM,* DoD 5220.22–M), as well as requirements for DIS employees.

Behavior patterns of possible significance include the following.

Attempts to expand access to classified information, through repeated volunteering for special assignments with additional access or inquiries concerning information for which the individual has no need to know.

Unauthorized removal of classified material from the work area, by making extra carbons or copies or placing of classified materials in briefcase, purses, gym bags, etc.

Repeated or unusual overtime, especially unaccompanied, whereby the individual arranges to be alone or unobserved in an office containing classified material.

Falsifying destruction records by requesting certification or witnessing signatures for destruction of classified materials which the individual has not actually seen destroyed.

Sudden, unexplained affluence as indicated by purchase of expensive cars, real estate, jewelry, etc.; by display of large amounts of cash; or by lump-sum repayments of significant debts, large stock purchases, or opening of substantial savings accounts—in the absence of some legitimate source of increased income. Unexplained affluence is of particular concern when it follows a period of leave or travel.

A pattern of recurring travel, within the United States or (especially) abroad, perhaps 2 to 4 times per year, without apparent recreational or business purpose. Married individuals who travel for tourism or recreation unaccompanied by family members may also be of concern.

Falsification of locations visited on leave statements or trip reports. Also reluctance to describe or ignorance concerning places supposedly visited.

Travel to Communist countries or on communist-flag ships or aircraft not involving an organized tour and not explained by business or family connections. Any attempts to visit communist countries without complying with applicable reporting requirements is of particular concern (e.g., paras. 5u and 6b[9], *ISM*).

Repeated association with Communist-country nationals without *bona fide* business purpose or without required reporting.

Note for contractors

Under the *ISM* cleared contractor employees must report anticipated contacts with communist-country nationals at professional meetings or through facility visits (para. 5u). A forthcoming change to the *ISM* (new para. 5ah, to be published in "Industrial Security Letter" no. 83L–1 and the next edition of the *ISM*) will require contractor employees to report "all questionable or suspicious contacts with nationals or representatives of communist countries," i.e., any contact "determined to consist of an actual, probable or possible hostile intelligence collection effort." Paragraph B, Appendix VII, is referenced for assistance in recognizing reportable contacts. (Para. 6c will be revised to require relaying of such reports from Security Supervisors to DIS and the FBI.)

Note of DIS employees

DIS employees, as well as all Federal employees, are required to report improper or suspicious contacts by representatives of any foreign interest, just as contractors are required to report. These naturally include contacts by communist-country nationals. See DIS Regulation 25–5.

While none of the indicators listed is proof of espionage, any pattern of conduct on the part of a cleared employee which suggests the possibility of improper activity should be reported by supervisors or managers to the Facility Security Supervisor (under para. 5af of the *ISM*). Security Supervisors should report in turn to the Defense Investigative Service and the FBI, as called for under paras. 6a(1), 6b(1) and 6c.

Where there is doubt whether information should be reported, it should be furnished to the proper authorities for evaluation. Security Supervisors should be aware that in two 1967 cases the U.S. Court of Appeals for the 4th Circuit held that a contractor is not liable for defamation of an employee because of reports made to the U.S. Government pursuant to the *Industrial Security Manual* (*Becker vs. Philco* and *Taglia vs. Philco*, 389 US 979). The Court stated in essence that such reports are privileged, since the contractor in executing the requirements of the *Manual* dons the cloak of a federal official.

Such reports do not of course constitute incrimination in themselves, and adverse action by government activities can only be taken with probable cause and due process. But the effectiveness of U.S. security and counterintelligence efforts is directly and vitally dependent upon early reporting of any possible instances of compromise or espionage.

64-268 O - 86 - 5

APPENDIX D

[From the Defense Security Institute Security Awareness Bulletin, December 1985]

PORTRAIT OF AN UNEASY SPY—CAVANAGH CASE HIGHLIGHTS THE VALUE OF GOOD SECURITY

Thomas Cavanagh had secrets to sell. And he made no bones about his motive. "I'm after big mony," he told the prospective buyers. "Before our relationship ends, I want to be independently wealthy."

He knew that espionage was a serious crime and knew about several people who had recently been arrested and gone to jail. But in order to clear up mounting debts, and make himself rich, the Northrop engineer was willing to take some chances.

"They're real security conscious [at Northrop] and all that crap," he remarked during one meeting at the Cockatoo Motel near Los Angeles. Cavanagh thought he knew how to get around the document controls and random searches at the plant, but he was still very worried about being caught.

What he didn't know was that he had already been caught. The "KGB agents" he was meeting with at the Cockatoo and the Lucky Lodge in Commerce, California were actually FBI undercover agents.

In December 1984, after three meetings monitored and recorded by the Bureau, Cavanagh was arrested and charged with espionage.

In May 1985 he was sent to prison for life.

The Thomas Cavanagh case has some comic sidelights, but also some serious lessons for counterintelligence and industrial security. For the most part it's a success story, both for the FBI, which caught him before he could get to the Soviets and for the security program which put some real curbs on his ability to damage the nation.

Some of the lessons are plain. Above all, the case points up the importance of document accountability and reproduction control. And it suggests that exit searches can be an effective deterrent to espionage activity.

In the first part of the article we'll set the scene and tell the story of Cavanagh's encounters with FBI undercover agents, who posed as KGB officers speaking Russian and broken English. We'll listen in on their conversations as Cavanagh discusses what he's up against at the Northrop plant and how physical security and document control are cramping his style as a spy.

Less straight-forward, as always, are the implications for personnel security: adverse information reporting and the psychological "profile" of the espionage offender. Follow-up investigation concluded that Cavanagh's supervisors had not neglected their reporting responsibilities and that the reporting program at his facility

was satisfactory—although there were some hints in his behavior that might seem obvious in hindsight.

There's no question about Cavanagh's main motivation. He wanted money, first to clear up current debts, then to make himself "independently wealthy." But his conversations with the undercover agents also hint at other contributing motivations—job dissatisfaction, disgruntlement with management, social and/or political resentments.

Investigation by the FBI and Defense Investigative Service after the arrest revealed further details about Cavanagh's background and personality—for instance, a fraudulent salary claim when he first came to work at Northrop and a pattern of impatience and indifference regarding rules and procedures.

In the second half of the article we'll look into Cavanagh's background, as revealed through these interviews with former managers, supervisors and coworkers. And perhaps glean some insights into what brought him to the Cockatoo Motel on that day in December, with a classified document stuffed inside his shirt.

SOME ASPECTS OF THE CAVANAGH CASE REMAIN CLASSIFIED

We can't discuss how he was originally detected and became involved in meetings with the undercover agents, since that would compromise important investigative methods. But it's significant to note—for the benefit of other would-be spies—that someone attempting to contact the KGB can end up in touch with the FBI instead.

And we can't discuss the information which Cavanagh was trying to sell. He didn't succeed in selling it, and obviously we don't want to give any of it away for free.

Suffice it to say that he was working on a classified project requiring Special Access, and he'd been put in for Top Secret clearance requiring a Background Investigation. He told the "KGB" that a substantial down payment on his information would insure that excessive indebtedness did not interfere with the clearance upgrade leading to even more sensitive access.

At the first meeting, on December 10, 1984, Cavanagh introduced himself to his contacts as Mr. "Peters."

Two topics dominated his conversation: his financial problems and worries about getting caught.

He said early in the first meeting: "I'm up for a Top Secret clearance rating but I won't get that clearance rating because of my bill problems.

"So somehow we have to come to an agreement, ah, on money." He needed several thousand dollars, he said, "just to get the bill collectors off my back."

"Peters" was worried about being caught partly because of the recent espionage cases which he had heard about. He mentioned Bell, Boyce and "the two people in Sunnyvale" (the Harpers).

He was worred about leaks "on your end," i.e., U.S. informants inside Soviet intelligence, no doubt thinking of the informants inside Polish intelligence who helped put Bell and Harper behind bars.

See appendix C on Bell and appendix B on Harper.

And he didn't want to talk with his contacts on the telephone—"because it's constantly being bugged; they bug it with microwaves."

But his biggest source of anxiety was the security program at Northrop.

He was extremely concerned about his accountability for documents. He wouldn't turn them over to the "KGB" agents, and he wanted to get them back to the plant as quickly as possible.

"I can't give you the documents and have them back in time. They have audits. A guy just came by today and asked me how many secret documents I have." Security might open his safe and check his documents at any time.

By sheer coincidence, Cavanagh had faced a surprise audit of his classified documents on the very day of this first meeting with what he thought was the KGB.

It was strictly a random check by a company security representative—who had no suspicion that the material he was reviewing was about to be put up for sale to the Soviets. Everything was in order, but Cavanagh had been visibly upset, according to coworkers interviewed after the arrest.

"What are you messsing around with me for? I've served my time in Vietnam," he told the security officer. Cavanagh obviously thought twice about what he was doing—although he went ahead and did it. But the system of strict accountability put some important limits on his espionage activities.

Cavanagh was also hampered by reproduction controls at Northrop. "You can't run you own copies in the plant. They got that regulated too." The agents had to bring in a camera and a portable copier and make copies in the motel room.

Northrop employees were subject to random search of anything handcarried in or out of the plant. And Cavanagh was worried about that as well. "I had to stick it in my shirt and walk out with it."

He couldn't always fit things under his shirt. But he thought he could get through the exit searches without detection. The searches, he believed, were sufficiently infrequent and predictable to be successfully avoided.

Tougher and tougher and tougher

When he arrived for a second meeting on December 12, Cavanagh was greeted warmly by his friends at the motel:

> "KGB": "So, how are you today?"
>
> CAVANAGH: "Good. But a little nervous because, ah, getting the documents out is getting tougher and tougher and tougher."
>
> "KGB": "Why tougher?"
>
> CAV.: "They're real security conscious, and all that crap. Okay?"
>
> "KGB": "So you were scared?"
>
> CAV.: "Well not scared, just very careful and apprehensive. . . . Every once in a while you get somebody that's real conscientious and wants to look at everything going in and out."

So the "triple threat" of document accountability, reproduction controls and random searches made Cavanagh a very nervous spy—very "careful and apprehensive," as he put it. (And an "apprehensive" spy is a certain sign of good security, although in this case it fell short of total deterrence.)

Cavanagh was unable to obtain documents without signing for them (though he tried to do so, as we will see).

Making "bootleg" copies was impossible. Northrop Advanced Systems Division controls document reproduction through a system of "fully-controlled machines." In other words, no self-service. Special operators handle all copying machines, under the oversight of security. They make sure that all requirements are met for authorization, marking and accountability.

Cavanagh was also worried about the entrance and exist searches. But he felt that they presented an acceptable risk.

He didn't get the chance to test this assumption over the long run. There's no way of knowing if he could have gotten past the guards throughout the "long-term relationship" which he hoped to establish with the KGB. But he, and perhaps others, had the *perception* that the search system could be beaten. It was a threat, but not enough of a threat.

"It's cash and carry

During the second meeting (December 12) Cavanagh pressed anxiously for quick payment. "It's cash and carry cause I'm in debt up to my ears. I'm after big money."

He wanted the several thousand dollars in two days, but the "Russians" wouldn't make any promises.

> CAVANAGH: "Is it, is it possible to see money by Friday [Dec. 14].
> "KGB": "By Friday, I don't know. By Christmas. . . ."
> CAV.: "Oh God."
> "KGB": "Oh, you have very, how you say Merry Christmas. If documents are good."
> CAV.: "To be honest with you gentlemen, I need it before the 25th for security reasons [the Background Investigation]. I need that money."
> "KGB": "Okay, we do our best."

They met again on December 18. Right away, Cavanagh asked about the money. The agents had the money. And an arrest warrant.

> "KGB": "So, ah, how do you do today? Good to see you."
> CAVANAGH: "Okay, okay. Any word on the cash?"
> "KGB": "Oh we got good surprise for you today."
> CAV.: "Okay, okay. Am I gonna get it today?"
> "KGB": "Da da, yes."

Cavanagh showed them the documents he had brought along, and they struggled to make the portable copier function properly. He spoke of his financial bind. He was bitter that he couldn't get a business loan for his AMWAY distributionship, while Vietnamese immigrants, he felt, easily got money for fishing operations.

The agents suggested that future meetings be held outside the United States. But Cavanagh didn't want to keep his documents out that long. Besides, unexplained foreign travel might "flag" his activities with security.

Cavanagh was a gun collector and showed the agents a .45 caliber pistol he was carrying, because he was "nervous." Earlier he had warned the "Soviets" against carrying firearms ("No guns, no guns, all right, no guns.") They discussed guns and hunting. One agent took the gun to admire it, and then quietly held on to it.

A long-term relationship

After copying the documents, the agents handed Cavanagh the payment in small bills. He counted it eagerly. He wanted to have monthly meetings, he said, with substantial payment each time.

It should be worth it to them, "because billions of dollars worth of research went into those drawings. Billions!" Of course he didn't want to be "too greedy." "You know, if we play it right, it's a long-term relationship."

Cavanagh complained that bill collectors were calling him at work. "It's demeaning, degrading, cause everybody knows your business, you know?" "Of course, must be problem," one agent sympathized.

Cavanagh added: "I'm bitter because I worked hard for the company and sometimes politics plays a big role in getting ahead."

As they finished their business Cavanagh heard a noise outside.

"It must be the maid, or perhaps the pipes," one agent said. "It wouldn't be bad just to look out the door," said "Peters." The agent looked out. "It is nothing."

But then a knock. The door was opened again. "FBI! Freeze, don't move!"

Cavanagh was arrested and charged with two counts of espionage. He was sentenced, on May 23, 1985, to two concurrent life terms in prison.

Postmortem

Espionage which threatens U.S. national security is never cause for celebration. But this case is, at least relatively, a success story. The F.B.I. caught Cavanagh before he reached the Soviets. And Northrop security did its job in curbing the range of his activities, through document accountability and control—and effective enforcement of need-to-know.

Particularly notable is the taming of the "Xerox" machine. Ready access to photo reproduction is popularly thought to have made document control obsolete.

But the copiers at Northrop were effectively controlled, so Cavanagh was forced to use original documents which were under accountability. This exposed him to detection through random audits, and it limited both the number of documents he could compromise and the length of time he was willing to keep them outside the plant.

Greed and indebtedness were the major motivations for Cavanagh. But there were other, more subtle, influences at work as well.

After the arrest, Cavanagh's activities, behavior and background were naturally probed in detail by both the FBI and Defense Investigative Service. We've already looked at Cavanagh's brief and very unsuccessful career as a spy.

What follows is the story of his career as a technician and engineer, with the U.S. Navy and three of the country's biggest aerospace companies. That career wasn't as successful as Cavanagh apparently thought it should have been.

Disappointment with his advancement both professionally and financially seems to have played a major role in the psychological lead-in to espionage.

Prologue

At the time of his arrest in late 1984, Cavanagh, 40 years old, was earning about $40,000 as an Engineer Specialist with the Advanced Systems Division of Northrop Corporation, Pico Rivera, California. He had begun his technical career as an Interior Communications specialist for four years in the Navy, leaving the service in 1967 as a Petty Officer Third Class. Between 1967 and 1978 he attended Cerritos Junior College, ultimately earning an Associate Degree.

He was married and had two sons, born in 1967 and 1968.

Rockwell and Hughes

He worked for North American Rockwell for about a year (July '68 to August '69) and then went to work for Hughes Aircraft Company, El Segundo, California. While at Hughes, Cavanagh was promoted from technician to "Research Associate." But he was unable to attain full status as an engineer without a four-year degree.

Records and recollections at Hughes didn't reflect anything particularly distinguished or out of the ordinary about Cavanagh. One supervisor recalled him as high-strung and temperamental but generally manageable. Another had found him likeable and easy to get along with.

But a third former boss said Cavanagh had problems dealing with people and recalled a heated argument in which he seemed on the verge of physical violence.

Cavanagh had once been formally counselled for tardiness and had been placed on a one-year probation for parking violations. His salary had been attached on three occasions, for debts of $125 or less.

He was very "money motivated," said one coworker. And he had a high opinion of his own skills and abilities. But he was unlikely to advance very far at Hughes, even apart from the lack of an engineering degree. Most coworkers assessed his professional abilities as fair-to-middling at best. His technical skills were "reasonably good," according to one supervisor. Another, more typically, rated him as a marginal electronics technician and better suited to mechanical assembly.

Cavanagh held a Secret clearance while working at Hughes.

Northrop: He hoodwinked us

In November 1981, Cavanagh made the jump to full engineer status when he joined Northrop Electronics Division in Hawthorne, Califorinia. Northrop gave him a substantial raise and the title of "Senior Engineer," on the basis of over ten year's experience as an electronics technician—and also due to Cavanagh's ability to sell himself despite a marginal record at Hughes.

But the size of the raise which Northrop gave him was based upon an inflated claim of final base pay at Hughes. Several co-workers at his former office were aware that he had presented Northrop with a pay slip reflecting substantial unitemized overtime, claiming the total amount as base salary for the pay period. Northrop Personnel Office accepted the claim, although one of Cavanagh's managers was pretty sure that he had "hood-winked us."

Cavanagh's Secret clearance was transferred from Hughes and he was assigned to work on automatic test equipment for the F-5 aircraft. At Northrop, Cavanagh generally held supervisory positions, even though here again his technical abilities were generally rated as marginal.

He had a "dynamic"—sometimes "brash"—personality, according to one coworker. His assertiveness evidently commended him to management as a potential leader, but it also led to some interpersonal problems on the job.

On his first assignment, supervising integration of test equipment for the F-5 project, Cavanagh's managers rated his engineering skills below par. One supervisor later recalled that he seemed better suited to a technician's role. He was "in over his head technically," said one coworker, but he had a "big ego" and "radiated confidence" in his own abilities.

Colleagues remembered him as a frequent complainer with a short temper. A couple of incidents had led to threatening remarks ("I'll knock her block off," and the like). Once he slammed a door into the back of a supervisor who was leaving the room after a heated exchange.

New assignment

In mid-1982 the F-5 project closed down and Cavanagh was given a less technically demanding assignment. One manager recalled that he took the downgrade in stride (there was no cut in pay), but he showed little enthusiasm for the new project. He was more "paper oriented" than the assignment required and "didn't like to get his hands dirty."

Part of his job involved computer maintenance, but he frequently called in the manufacturer's technician without really trying to fix a problem himself. Cavanagh viewed himself as a supervisor, one manager remarked, when the job really called for a "doer."

Managers and co-workers had seen no signs of major financial difficulties while Cavanagh worked in the Electronics Division. He wore good clothes and had a gun collection and two Corvettes (mid-70's vintage)—but nothing really out of line for someone making in the neighborhood of $40,000 per year. He asked for an early paycheck on a couple of occasions. During 1982 he took about $1000 as an advance on a trip to Beaverton, Oregon for a technical training

course. He apparently had trouble repaying what was due when he returned and was contacted several times by the finance office. He sometimes complained casually about owing money to unspecified creditors. But, in all, his co-workers had no reason to suspect substantial problems.

Cavanagh was separated from his wife at about this time (1982). He had no really close friends at Northrop and co-workers were unsure about the exact timing and details of his marital difficulties. But it was generally known that he had begun an affair with another woman during the trip to Oregon. After he moved out of the family house, the Beaverton woman came down to California to live with him in an apartment.

In January of 1984 Cavanagh was transferred on loan with several other engineers to an urgent and sensitive project in Northrop's Advanced Systems Division (ASD) in Pico Rivera. Cavanagh was one of the first to be chosen to go, according to one manager. Supervisors had agreed that he was more troublesome personally than he was worth technically.

Last stop

And again at ASD he ran into personal difficulties and soon had a reputation as a "chronic complainer." He had at least one heated exchange with his first supervisor, and co-workers recalled other "loud and nasty" remarks. He frequently objected that others were receiving promotions and raises while he was getting less than his due.

A subsequent supervisor at ASD recalled that Cavanagh was careless and impatient with controls and procedures and had an inflated view of his own capabilities. But this manger thought Cavanagh might respond to additional responsibility, so he placed him once again in a supervisory position, as a lead engineer—his final assignment prior to the arrest in December 1984.

ASD management personnel interviewed after the arrest suggested that Cavanagh had some problems with administration and working with others but was improving in those areas. Again his engineering skills were called into question, but he seemed to be meeting basic expectations.

In this last assignment Cavanagh seemed to be generally well-liked by co-workers and subordinates. He regularly bowled and played softball with groups from the office.

One engineer who worked for him said that Cavanagh was the "clown" of their group. Everyone had laughed when, shortly before his arrest, he asked if he could deposit $10,000 in a bank without alerting the IRS.

Financial brinksmanship

Co-workers at ASD had a general idea that Cavanagh was financially pressed. Most attributed this to his separation and divorce. One colleague recalled being mildly surprised when Cavanagh bought another car (1984 Blazer). He was upset in November 1984 about a raise which he considered inadequate. At about that time he had asked the company to pay him a $3000 referral bonus for his own employment. (They didn't.)

One colleague remembered that Cavanagh seemed to have a lot of credit cards. And a couple of people mentioned a recent two-week Club Med vacation in Mexico.

Cavanagh complained to the undercover agents that "everybody" knew his business. But in fact no one had any idea of the extent of his indebtedness.

When investigators reviewed Cavanagh's financial records, they found about 25 outstanding credit accounts, including two American Express cards (one green, one gold), two Master Card accounts and five Visa cards. In December 1984 his balance with Club Med was almost $17,000.

Overall, he owed more than $41,000, in addition to a $98,000 mortgage. He had managed to make most of his payments so far, and none of the creditors had yet taken legal action. But there were several past due notices and he clearly had more debt than he could manage for much longer.

Looking for loopholes

Several former supervisors remarked that Cavanagh often tried to "test" the system, to see how far he could bend the rules. But he generally fell into line when counselled or confronted.

This pattern held true in his handling of classified material. At the Advanced Systems Division Cavanagh regularly obtained classified documents from two control stations. The document control people at both locations remembered having trouble with him. He would often pull documents from the cabinet himself, which many employees did during busy periods.

But Cavanagh would sometimes try to walk out without signing a receipt. When challenged he would plead absent-mindedness or simply treat the process as a joke.

The control clerks learned to keep an eye on him. And they apparently succeeded in keeping tabs on his documents. All the classified items which Cavanagh handed over to the undercover agents were duly signed for—hence his anxiety to get them back to the plant as quickly as possible.

Cavanagh's attempts to disregard and dismiss security requirements are typical of an attitude which is frequently encountered, perhaps most frequently among senior executives or "technical types" who feel they have a claim to special exemption from the rules.

Security Awareness Bulletin #2-85 (December 1984) describes several cases of this kind, in an article entitled "Above the Law." These were cases of security violations which did not—so far as we know—involve actual espionage. But they still involved compromise and potential damage to national security.

Cavanagh was not allowed to circumvent the system. But his case is a reminder of just how dangerous this kind of attitude can be.

No easy answers

The "typical" spy has yet to be discovered and the behavioral profile that will let us recognize one every time has yet to be invented. The psychology of espionage is not a source of tidy conclusions.

But Cavanagh shows some traits which we've encountered before in other spy cases. Job and career dissatisfaction is a big one, especially when it involves a sense of resentment toward the organization. Financial difficulties and/or irresponsibility are old standbys. Cavanagh, in addition, showed some tendency to violent or disruptive behavior, some instances of dishonesty and a general lack of respect for authority and procedural process.

Still, none of this rose to the level where supervisors considered reporting it for security purposes. Cavanagh was not a model citizen, but his behavior was well within normal, or at least tolerable, limits—until, quite suddenly by all indications, he went over the edge and tried to sell out the country to make himself rich.

How do we distinguish the Cavanaghs, *before* the fact, from the many other cleared people who are simply having difficulties with life's normal trials and tribulations?

Unfortunately, we don't often distinguish them, until after the fact. And we can't—until and unless we know a lot more about human psychology.

But we *can* protect the documents and the information, as Northrup did, by applying the proper measures for accountability and control, as well as physical safeguards. None of that will prevent espionage. A clearance, like any other kind of trust, always carries the potential for betrayal. But controls can make spying a lot tougher and a lot more expensive and a lot more risky.

Mr. Cavanagh took the risk and lost. He'll be in prison for a long time. Others will be that much more reluctant to take the same chances.

Appendix E

United States District Court, Eastern District of New York and Southern District of New York

United States of America

AGAINST

1. Gennadiy Fedorovich Zakharov, defendant,

2. Premises Known and Described as the Second Floor Apartment of a Two-Family Residence Located at 6019 Tyndall Avenue Bronx, New York; and

3. One 1982 Blue Plymouth Reliant Bearing New York License Plate 2281-ASJ

Affidavit for an Arrest Warrant and Search Warrant

(T. 18, U.S.C. § 794(c))

Eastern District of New York, Southern District of New York, *ss:*

Daniel K. Sayner, being duly sworn, deposes and says that he is a Special Agent of the Federal Bureau of Investigation, duly appointed according to law and acting as such.

In or about and between April 1983, to and including the date of this affidavit, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant Gennadiy Fedorovich Zakharov (hereinafter "Zakharov") did knowingly and willfully combine, conspire and agree together with others known and unknown, to communicate, deliver, transmit and attempt to communicate, deliver and transmit to a foreign government, to wit, the Soviet Union, directly and indirectly, documents, writings, code books, instruments and other information relating to the national defense with the intent and reason to believe that it was to be used to the injury of the United States and to the advantage of a foreign nation, in violation of Title 18, United States Code, Section 794(a).

OVERT ACTS

In furtherance of the conspiracy and to effect the objects thereof, the following overt acts, among others, were committed in the Eastern District of New York and elsewhere:

1. On or about May 10, 1986, the defendant Zakharov met with a confidential source (hereinafter "CS") in Queens, New York, and entered into an agreement with "CS" whereby "CS" would be re-

quired to obtain classified information relating to the national defense for Zakharov and the Soviet Union. The defendant Zakharov made a payment to "CS" of a sum of money at this meeting.

2. On or about August 2, 1986, the defendant Zakharov met with "CS" in Queens, New York, and assigned "CS" the task of surreptitiously copying documents kept in a locked safe at "CS's" place of employment, a manufacturer of precision components for use in the engines of military aircraft and in radars, so that Zakharov could determine the importance of the information contained in the documents.

(Title 18, United States Code, Section 794(c))

Upon information and belief, there is presently concealed within the premises known and described as: (1) The second floor apartment of a two family residence located at 6019 Tyndall Avenue, Bronx, New York (hereinafter the "Premises") and (2) One 1982 blue Plymouth Reliant bearing New York license plate 2281-ASJ property; namely, 1) espionage paraphernalia including a) devices used to conceal and transmit classified and intelligence information; b) materials utilized by espionage agents to communicate among each other and with a foreign government; to wit, coded pads; secret writing paper; greeting cards and other documents containing microdots; microfiche and instructions in the use of the materials; recording and electronic transmittal equipment; and c) chemicals used to develop coded or secret messages; 2) books, records, documents and papers which reflect a) identities of foreign espionage agents; b) financial transactions including payments made to foreign espionage agents; c) telephone records reflecting contact among foreign espionage agents; 3) fingerprints of various persons who have visited or been at the Premises; and 4) other documents and paraphernalia that refer or relate to Zakharov's activities as an espionage agent. The aforedescribed property constitutes evidence of a violation of Title 18, United States Code, Section 794(c), to wit, conspiracy to transmit, deliver and communicate documents and information relating to the national defense to a foreign government with the intent or reason to believe that it is to be used to the injury of the United States and to the advantage of a foreign nation.

The source of your deponent's information and the grounds for his belief are:

1. "CS" is an individual known to your deponent to be a confidential source working for the Federal Bureau of Investigation. "CS" has provided information to your deponent for approximately the last one and one-half years regarding the defendant Zakharov's contacts with "CS" and has provided information to other agents since in or about April of 1983 regarding the defendant Zakharov's contacts. The majority of the meetings between the defendant Zakharov and "CS" described below which occurred from March of 1985 to August 2, 1986 have been tape recorded. The recordings corroborate "CS's" accounts of his meetings with Zakharov. In addition, surveillance agents of the Federal Bureau of Investigation have observed numerous meetings between Zakharov and "CS".

2. "CS" has informed agents of the Federal Bureau of Investigation that in April 1983, "CS" was approached by Zakharov on the campus of Queens College, New York, where "CS" was a third-year student majoring in computer sciences. Zarharov did not identify himself as a Soviet, but did tell "CS" that he worked at the United Nations doing scientific research. Zakharov requested "CS's" help in obtaining material of robotics and computer technology. Zakharov offered to pay "CS" a sum of money for "research time" necessary to obtain unclassified microfiche from local university libraries. At this first meeting Zakharov gave "CS" a list of specific microfiche relating to robotics and computers that "CS" was to obtain for Zakharaov. A second meeting was scheduled.

3. On or about May 3, 1983, a second meeting occurred between "CS" and the defendant Zakharov. During this second meeting, Zakharov identified himself as a Soviet and paid "CS" a sum of money even though "CS" had not located any material for Zakharov.

4. During the period from May 1983 to March 1985, Zakharov met with "CS" on numerous occasions, most often in Queens, New York, but also occasionally in Brooklyn, New York. In compliance with Zakharov's instructions during this period of time, "CS" would steal unclassified microfiche from various libraries and information centers and provide the microfiche to Zakharov. Zakharov continued to pay "CS" for his services.

5. As "CS's" graduation from Queens College approached in January 1985, the defendant Zakharov regularly encouraged "CS" to apply for a job with a high tech company. Zakharov paid "CS" to have professional résumés prepared to assist "CS" in obtaining such employment. Additionally, Zakharov advised "CS", in substance, that the Soviets would be willing to pay for educational expenses if "CS" wanted to go to graduate school.

6. During the period from in or about March 1985 through in or about May 1985, the defendant Zakharov discussed with "CS", among other topics, emergency meeting procedures, development of drop sites for the transfer of documents between Zakharov and "CS", and emergency signaling procedures. Zakharov further advised "CS", in substance, that he wanted to have a longterm relationship with "CS" and that "CS" should not be in this type of activity entirely for money but also to hurt America.

7. In or about September 1985, "CS" became employed at a company located in Queens, New York (hereinafter the "Company"). The Company manufactures unclassified precision components for use in military aircraft engines and in radars that are assembled by major defense contractors such as the Bendix Corporation and General Electric Corporation.

8. After "CS" began working for the Company, Zakharov's emphasis in the gathering of information shifted from seeking unclassified microfiche on technical subjects such as robotics, computers and artificial intelligence to seeking documents from the Company relating to the Company's manufacturing activities. For instance, on or about January 18, 1986, Zakharov instructed "CS" to photocopy the first few pages of the operating manuals for the machines that the Company uses to manufacture its military aircraft components. Zakharov stated to "CS", in substance, that by knowing the

type of machines the company uses, his "Institute" would be able to determine specifically what the Company manufactures. Zakharov also cautioned "CS" at this time that their relationship was no longer as innocent as it had been previously and that no one should know of their relationship. Your deponent believes that the "Institute" is a term that Zakharov uses to refer to his superiors in the United States and Moscow.

9. On or about March 15, 1986, the defendant Zakharov met with "CS" in Queens, New York. At this meeting, "CS" provided Zakharov with unclassified documents pertaining generally to the maintenance and manufacture of components of military aircraft engines. At this meeting, Zakharov asked "CS" if any materials at the Company to which he might have access were classified. Zakharov further discussed with "CS", in substance, whether "CS" would like to enter into an agreement with Zakharov pertaining to their clandestine relationship. At this meeting, Zakharov made payment of a sum of money to "CS".

10. On or about April 20, 1986, Zakharov met with "CS" in Queens, New York. At this meeting, Zakharov stated, in substance, that before Zakharov could make payment to "CS" for delivery of documents and information, Zakharov would first have to send the material to Moscow for their review.

11. During a meeting on May 10, 1986, which occurred on a subway platform in Queens, New York, Zakharov dicated an agreement to "CS" whereby "CS" would continue to work for the Soviets for a period of ten years, after which the agreement could be reconsidered and renegotiated. The agreement dictated by Zakharov to "CS" specifically included a provision that "CS" would be required, as part of his assignments, to obtain classified material for the Soviets which could not be obtained by a citizen of the USSR. The agreement entered into between Zakharov and "CS" further provided that the amount of payment to "CS" for his services would be based on the quality and quantity of the information provided by "CS". As Zakharov dictated the agreement, "CS" wrote it out on a piece of paper. "CS" then signed the agreement and handed it to Zakharov who retained possession of the agreement. Zakharov made a payment to "CS" of a sum of money at this meeting.

12. On or about May 31, 1986, the defendant Zakharov again met with "CS" in Queens, New York. During this meeting, Zakharov asked "CS", in substance, if any of the documents maintained in the Company's safe were stamped confidential or were restricted in any manner. Zakharov further urged caution on the part of "CS" in entering the Company's safe. Zakharov also requested that "CS" remain unmarried.

13. Shortly after this meeting, the defendant Zakharov travelled to the Soviet Unon where he remained until on or about July 20, 1986.

14. Upon Zakharov's return to the United States, he again met with "CS" in Queens, New York on or about August 2, 1986. At this meeting, Zakharov told "CS" that the "Institute" recommended that "CS" attend Queens College initially and then transfer to Brooklyn Polytechnic Insitute at a later time. Zakharov further stated, in substance, that he would pay "CS" a sum of money for graduate school plus additional expenses at their next meeting.

15. Also during this meeting of August 2, 1986, the defendant Zakharov sought more information from "CS" about "CS's" employment and, specifically, about the safe located at the Company. "CS" informed Zakharov that he had seen documents in the safe that bore the designations "(C), (U) or (O)," but that "CS" did not know what these designations meant. Zakharov instructed "CS", in substance, to attempt to copy some of the documents in the safe so Zakharov could determine if the material was important.

16. Investigation has disclosed that the defendant Zakharov currently resides at the premises and has resided there for over three years. On two occasions in 1986 on which Zakharov met with "CS", surveillance agents first observed Zakharov depart from the premises carrying a shoulder-strap gym-style bag. On both occasions, Zakharov was observed entering a 1982 blue Plymouth Reliant bearing New York license plate 2281-ASJ and driving off. On one of these occasions surveillance agents followed Zakharov and observed Zakharov drive the Plymouth Reliant to a location, park, exit the car and walk in the direction of a subway station, all the while carrying the shoulder-strap gym-style bag. On both of the occasions on which Zakharov was observed leaving the premises, Zakharov subsequently arrived at the designated meeting place carrying what appeared to be the same shoulder bag and met with "CS". Also on various occasions, Zakharov has mentioned to "CS" that he (Zakharov) has parked his car in Manhattan prior to meeting with "CS". Zakharov uses the shoulder bag to conceal documents provided to him by "CS" at their meetings. In your deponent's experience, automobiles used by espionage agents often contain counter-surveillance devices, such as scanners.

17. Investigation by agents of the FBI has determined that the defendant Zakharov is employed in the United States as a Scientific Affairs Officer assigned to the Center for Science and Technology for Development at the United Nations Secretariat in New York. He has been in the United States since in or about December 1982.

18. Your deponent has been assigned to the Foreign Counterintelligence Squad in New York City for the past two years. During this period of time, I have worked on more than a dozen cases involving Soviet and East European intelligence service operations and have therefore become thoroughly familiar with tactics, methods and operational techniques of the intelligence services of these countries. In your deponent's experience, and based on information provided to your deponent by other officials in the Foreign Counterintelligence area, Soviet and East European Intelligence agents utilize espionage paraphernalia including devices designed to conceal and transmit classified and intelligence information, materials used by espionage agents to communicate among each other and with a foreign government to wit, coded pads, secret writing paper, greeting cards and other documents containing microdots, microfiche together with instructions in the use of these materials, recording and electronic transmittal equipment, chemicals used to develop coded or secret messages; and books, records, documents and papers which reflect: a) the identities of foreign espionage agents; b) financial transactions including payments made to foreign espionage agents; and c) telephone records reflecting contact

among foreign espionage agents. It is also your deponent's experience that these materials are kept in safe houses and residences used by intelligence agents. Based upon the facts set forth above, it is your deponent's belief that the defendant Zakharov is a Soviet intelligence agent conducting espionage activities in the United States. Moreover, the investigation has established, as described above, that the premises known and described as the second floor apartment of a two-family residence located at 6019 Tyndall Avenue, Bronx, New York and one blue 1982 Plymouth Reliant bearing New York license plate 2281-ASJ are being used by an agent of Soviet Intelligence in the conduct of his espionage activities.

19. Agents of the Federal Bureau of Investigation presently plan to arrest the defendant Zakharov on Saturday, August 23, 1986, after he has received the latest batch of documents from "CS". It is anticipated that the arrest will occur on or after 4:00 p.m. on Saturday. Your deponent fears that confederates of the defendant Zakharov will be warned of the arrest when Zakharov fails to return promptly from the meeting and may attempt to destroy evidence of the conspiracy at the location to be searched. Therefore, your deponent requests that authority be given for agents to execute the warrant at any time of the day or night.

Wherefore, your deponent respectfully requests (1) that a warrant issue for the arrest of the defendant Gennadiy Fedorovich Zakharov, so that he may be dealt with according to law; (2) that a warrant issue allowing your deponent or any Special Agent of the FBI with proper assistance to enter at any time of the day or night the premises known and described as the second floor apartment of a two-family residence located at 6019 Tyndall Avenue, Bronx, New York and therein to search for property; namely, 1) espionage paraphernalia including a) devices used to conceal and transmit classified and intelligence information; b) materials utilized by espionage agents to communicate among each other and with a foreign government to wit, coded pads; secret writing paper; greeting cards and other documents containing microdots; microfiche and instructions in the use of these materials; recording and electronic transmittal equipment; c) and chemicals used to develop coded or secret messages; 2) books, records, documents and papers which reflect a) identities of foreign espionage agents; b) financial transactions including payments made to foreign espionage agents; c) telephone records reflecting contact among foreign espionage agents; 3) fingerprints of various persons who have visited or been at the apartment; and 4) other documents and paraphernalia that refer or relate to Zakharov's activities as an espionage agent.

DANIEL K. SAYNER,
Special Agent, Federal Bureau of Investigation.

Sworn to before me this 22nd day of August, 1986.
United States Magistrate, Eastern District of New York.

APPENDIX F

United States
Information
Agency

Washington D.C. 20547

April 29, 1986

USIA

Senator David Durenberger
375 RSOB
Washington, D.C. 20510

FORGERY

Dear Senator Durenberger:

Now that there is conclusive evidence that [illegible] breakdown of a Chernobyl nuclear power plant reactor produced a considerable quantity of radioactive fallout, we have a chance to utilize this fact for propaganda purposes. Furthermore, it is good for us that Moscow has made no official statement on the event.

Therefore we suggest that following steps should be taken:

- Reports should be spread by our associates in European information media giving the public the details of Chernobyl disaster:

- number of victims should be alleged to be somewhere between 2,000 and 3,000;

- mass evacuation of population from the 100-mile zone;

- transport problems, shortage of various goods, chaos, and panic should also be given publicity;

- appropriate illustrations and textual material should be provided;

- campaign should be organized by USIA officials who should also supply the material needed.

- In view of the forthcoming Tokyo summit data should be provided for the statement on the Chernobyl disaster to be issued by the seven leaders.

- Considering the facts about the increased air pollution, our allies should be recommended to stop imports of food and other commodities from Eastern bloc.

- Our allies should be influenced so as to make a request for compensation for contamination of their territory.

We will keep you informed of any future measures.

Best regards,

Herbert Romerstein

Herbert Romerstein
Senior Policy Officer
on Soviet Active Measures

United States
Information
Agency

Washington, D.C. 20547

USIA

August 16, 1985

Dear General Schweitzer:

Enclosed is a copy of the forgery attributed to you.

We are able to draw some conclusions at this time.

1. The copy of the forgery in our possession was placed on the desk of an Italian journalist by an unknown person. It was in a plain white envelope. This method of surfacing a forgery is a well-known Soviet technique.

2. Based on information supplied by General Schweitzer, USIS Rome was able to convince the journalist that the letter was a forgery. As a result the perpetrators were compelled to use a Guatemalan "news service" known to be associated with the Cuban-Nicaraguan-backed insurgents to provide credibility to the Italian news agency that surfaced the forgery. This revealed the Cuban-Nicaraguan hand in the forgery.

3. General Schweitzer's evidence, provided to the Italian press service, was widely distributed both by them and USIA. Thus, the facts about the forgery are now well-known. Such exposes raise the cost to the forgers.

The following are preliminary findings of an unofficial but expert forensic examination of the forgery:

1. Paper: Not common in America.

2. Text: Possibly, the letterhead and the text were all printed on one machine, although it is difficult to determine from a copy. The letterhead does not appear to be "spliced" on.

3. Signature: Because the letter is a photocopy and the note provided was signed with a felt-tip pen it is difficult to say anything about the signature. However, it appears to be well executed. Lab would need several samples of the General's signature to determine such things as where he signs his name in relation to the signature bloc.

4. Comments: Based upon a cursory examination, it appears the document is an excellent forgery.

A linguistic examination of the forgery is now being done.

Lt. General Robert L. Schweitzer
Inter-American Defense Board
2600 16th St., N.W.
Washington, D.C. 20441

I am sorry that I did not get back to you earlier on this matter. We will continue to pursue this forgery and will keep you advised as we gain additional information.

Best regards,

Herbert Romerstein
Senior Policy Officer
on Soviet Active Measures

Enclosure: Letter

INTER-AMERICAN DEFENSE BOARD
2600 - 16th Street, N.W.
Washington, D.C. 20441

25 de febrero de 1985

Su Excelencia
Augusto Pinochet Ugarte
Presidente de la República de Chile
Cap. Gral. del Ejército
Palacio de la Moneda
Santiago

FORGERY

Estimado Sr. Presidente:

Me complace informar a Su Excelencia que la entrega a Chile del nuevo armamento solicitado será decidida en el más corto plazo. Me ha causado agrado el saber, a través del Sr.Motley, que usted ha mostrado vivo interés por ampliar nuestra cooperación en el terreno militar. Estimamos su profunda comprensión de las particularidades de la nueva situación internacional y de las iniciativas del presidente Reagan, encauzadas a fortalecer nuestra capacidad defensiva común.

Quisiera asegurar a Su Excelencia que seguirá usted contando con nuestro decidido apoyo en sus esfuerzos por fortalecer la libertad y la democracia en Chile.

Con respecto a nuestras acciones conjuntas en América Central, quisiera sugerirle la conveniencia de que las primeras unidades chilenas sean trasladadas a El Salvador y Honduras ya en marzo. Nuestros representantes en dichos países recibirán instrucciones dentro de dos semanas. Junto con su representante trataremos los demás problemas de nuestra cooperación en una de las próximas reuniones de la JID.

Con los mejores testimonios de mi más alta consideración y estima personal hacia Su Excelencia, saluda a usted

Muy atentamente,

Robert L. Schweitzer
ROBERT L. SCHWEITZER
Lieutenant General, U.S. Army
Presidente

APPENDIX G

DRAFT SENATE SECURITY MANUAL

FOREWORD

The United States Senate is obligated to safeguard the classified information we obtain and produce as a result of our legislative activities. To ensure that the Senate lives up to its obligations, this manual is published to establish uniform security practices within the Senate.

TABLE OF CONTENTS

	Page
SECTION I. GENERAL	146
1. Scope	146
2. Designation of Senate Office of Security	147
3. Reports	147
SECTION II. HANDLING OF CLASSIFIED INFORMATION	147
1. Policy	147
2. Classification	147
3. Marking Classified Material	148
4. Record of Classified Material	148
5. Inventory/Accounting of Classified Material	149
6. Special Requirements for Secret and Top Secret	149
7. Storage and Certification	149
8. Safeguards During Use	150
9. Transmission	150
10. Reproduction	150
11. Exemptions	151
SECTION III. PERSONNEL SECURITY	151
1. General	151
2. Clearance Standards for Senate Staff	151
3. Investigative Requirements	151
4. Consultants or Contract Personnel	152
5. Denials and Terminations of Security Clearances	152
6. Reinvestigation and Revalidation Program	152
7. Secrecy Agreements	152
8. Security Violations	153
9. Penalties for Breaches of Security	153
10. Security Education and Awareness	153
11. Termination of Security Clearances, Employment, or Extended Leave	154
12. Security Responsibilities in Personal and Committee Offices	154
13. Foreign Travel	154
14. Contact Reports	155
GLOSSARY	155

SECTION I. GENERAL

1. *Scope.* This manual establishes the requirements for safeguarding classified information to which employees of the United States Senate have access or possession. The manual is written in terms of the most common situations where the employee has access to, or possession of, classified information in the performance of assigned duties. It is the responsibility of every employee of

the Senate to be familiar with security requirements and to comply with them. If you have any questions regarding the proper safeguarding of classified information, or any problems relating to security matters in general, contact your office security manager for guidance and direction before you act.

2. *Designation of Senate Office of Security.* In order to insure that all Senate offices handle classifed information in a uniform and acceptable way, an Office of Senate Security has been created under the auspices of the Senate Majority Leader. The duties of the Director of the Senate Office of Security shall include the following:

a. Function as a central point within the Senate for the receipt, control, transmission, storage, and destruction of classified material.

b. Process clearance requests for personnel of the Senate.

c. Provide centralized recording and certification of clearances held by Senate personnel.

d. Administer a security awareness program, including security briefings and debriefings for the benefit of all Senate personnel.

e. Consult on security issues with Senate offices and conduct security surveys, inspections, and audits.

f. Conduct security liaison, both internal and external, on behalf of the Senate.

g. Such other duties related to personnel and document security which the Majority Leader may direct.

3. *Reports.* The Director of Security shall immediately submit in writing to the Majority Leader a report of any loss or compromise of classified material or information, or any other serious breach in Senate security procedures which merits the attention of the Majority Leader.

a. An annual report shall be provided to the Majority Leader on the number of security violations which resulted in disciplinary action being taken against Senate employees.

b. An annual report shall be provided to the Majority Leader on the number and types of clearances held by Senate employees.

SECTION II. HANDLING OF CLASSIFIED INFORMATION

1. *Policy.* Executive Order 12356 provides a uniform system for classifying, declassifying, and safeguarding national security information. This order assigns original classification authority to certain members of the Executive branch. Classified material originated by the Executive branch and under the custodial control of the Senate will be handled and safeguarded in accordance with the provisions of E.O. 12356 and this manual.

2. *Classification.* The assignment of classification involves a determination of the degree of protection certain information requires in the interest of national security. There are three categories of classified information: Top Secret, Secret, and Confidential. Classification of material may be supplemented by special designations and access requirements. Definitions of classification designations and other supplemental access designations may be found in the glossary of this manual.

3. *Marking Classified Material.* The originator of material which contains classified material is responsible for properly marking the security classification of the material. Classification designation by conspicuously marking serves to warn the holder what degree of protection is required for that information or material. Other notations facilitate downgrading, declassification, and aid in derivative classification actions. Therefore, it is essential that all classified material be marked in such a manner that it is clear to the holder what level of classification is assigned to the material. Although not required by this manual, those who originate material which contains classified information are urged to classify individual paragraphs within a document if deemed necessary.

a. The markings shown in paragraphs (1) through (4) below are required for all classified information. Some material, such as documents, letters, and reports can be marked easily with the appropriate markings. Marking other materials, such as ADP media and slides, will be more difficult due to size or other physical characteristics. Since the purpose of the markings is to warn the holder that the information requires special protection, it is necessary that all classified material be marked with the appropriate markings to the fullest extent possible to ensure it is afforded the necessary safeguards.

(1) *Identification Markings.* All classified material shall be marked to show the office responsible for its preparation, and the date of preparation. These markings are required on the face of all classified documents.

(2) *Overall Markings.* The overall classification of a document, or any copy or reproduction thereof, shall be stamped at the top and bottom on the outside of the front cover (if any), on the title page (if any), and on the outside of the back cover (if any).

(3) *Page Markings.* Interior pages of classified documents shall be stamped at the top and bottom with the highest classification of the information appearing thereon, or with the overall classification of the document.

(4) *Additional Markings.* In addition to the markings specified above, classified material shall be marked, if applicable, with one or more notations which indicate the material is further restricted to special access categories (e.g.. Restricted Data notation and Dissemination and Reproduction notices).

4. *Record of Classified Material.* a. *Accountability Records.* The security manager of each Senate office shall maintain an accountability record of all Top Secret and Secret material, and special access materials regardless of classification. The record shall include all such classified material received or produced by, or in the custody of, the office and shall reflect as a minimum:

(1) The date of receipt.

(2) The classification of the material.

(3) The office which originated the material.

(4) The Senate Office of Security or Committee control number.

(5) A brief unclassified description of the material.

(6) The disposition of the material and date thereof (e.g., file location, or return to the Senate Office of Security).

5. *Inventory/Accounting of Classified Material.* When directed by the Director of Security (approximately on a semi-annual basis), each Senate office shall make an inventory and accounting of all Top Secret and Secret material, and special access materials, and shall submit a report to the Director of Security. The inventory and accounting shall consist of the actual sighting of each item listed in the accountability records. The report of each office's holdings will then be checked against the records of the Office of Security to insure proper disposition has been made for all accountable classified holdings.

a. *Receipt of Classified Material.* As a matter of practice, all classified material destined for Members' offices should be received by the Senate Office of Security. In the event classified material is received by a Member's office directly, it should be taken to the Office of Security within one working day to be properly receipted for and brought under Senate control procedures.

b. *Production of Classified Material.* When an office produces Top Secret or Secret material, and special access materials, such documents must be registered with the Office of Security within one working day.

c. *Semi-Annual Review of Classified Material.* For the purpose of reducing to a minimum the quantity of classified material on hand at any given time, each Senate office shall establish a program for the semi-annual review of classified material. All Senate offices wishing to dispose of classified information or place it in long-term storage may forward it to the Office of Security (using proper receipting procedures) who will assume responsibility for the proper storage or destruction of same.

6. *Special Requirements for Secret and Top Secret.* It is essential that an up-to-date record be maintained of all persons who are afforded access to Secret and Top Secret information. A record shall be maintained with each item of Secret and Top Secret material that shows the names of all individuals given access to the item and the date (or inclusive dates) on which access by each individual occurred. Such record shall be retained in the Office of Security for a period of three years from the date the material was destroyed, dispatched outside the Senate, declassified, or downgraded to less than Secret.

7. *Storage and Certification.* Classified material must never be left unattended. It must be secured in an approved storage container or under direct surveillance of an authorized person at all times. Senate offices will not be eligible to receive or store classified material until they have been certified by the Director of Security as having adequate storage capability. Classified material, when not in actual use, shall be stored as follows:

a. *Top Secret and Special Access—Cabinets and Vaults.* Top Secret and Special Access material shall be stored in a General Services Administration (GSA) approved security filing cabinet bearing a GSA Test Certification label or in a Class A vault constructed in accordance with the requirements of the Department of Defense Industrial Security Manual.

(1) Entry to the room in which the container or vault is located shall be controlled by a properly cleared employee so as

to control admittance to the room during normal working hours.

(2) During non-duty hours the room in which the container or vault is located shall be patrolled and each container or vault inspected by a Capitol Police Officer at least once during each four-hour period. The inspection procedure will be supervised by a system which provides a written record of the coverage.

b. *Secret and Confidential Cabinets.* Secret and Confidential material may be stored in a Top Secret cabinet or vault, or in a steel file cabinet secured by a steel bar and the three-position changeable combination padlock.

c. *Supervision of Storage Containers.* Only a minimum number of authorized persons shall possess the combinations to the storage containers or vaults, or have access to the information stored therein. To facilitate investigation of a container found open and unattended, a record shall be maintained by the Office of Security of the names, home phone numbers, and addresses of persons having knowledge of the combination. In addition, the combinations of storage containers in Members' offices shall be maintained, in a sealed envelope, by the Office of Security. Such envelope may be opened only at the direction of the Member or the office security manager. Cabinets and vaults in which classified information is stored shall be kept locked when not under the direct supervision of an authorized person entrusted with the combination or the contents.

d. *Alternate Storage Location.* The Office of Security shall maintain a list of all approved classified storage cabinets and vaults within the Senate. Each cabinet or vault listed shall be identified by location. In the event a cabinet or vault become damaged or inoperable in a Senate office, the Office of Security will provide temporary secure storage until such time the cabinet or vault is restored to good repair.

8. *Safeguards During Use.* Classified information is provided to a properly cleared person on the basis of a need-to-know. Determination of a need-to-know is an individual responsibility. Before divulging any classified information, Senate employees shall make certain of the recipient's identity, level of clearance, and need-to-know. The Office of Security will maintain a list of Senate employees whose level of clearance has been properly established. Classified materials, when not safeguarded as provided for in paragraphs 7a and 7b, and when in actual use by cleared personnel, shall be protected as follows:

a. Kept under the constant surveillance of an authorized person, who is in a physical position to exercise direct security controls over the material.

b. Covered, turned face down, placed in storage containers, or otherwise protected, when unauthorized persons are present.

c. Returned to storage containers as soon as practical after use.

9. *Transmission.* Transmission of classified material from Senate offices to any other Senate office, government agency, or other authorized recipients shall be registered with the Office of Security.

10. *Reproduction.* All reproductions of classified material shall be marked or stamped with the same classification as the original. Re-

production of classified material shall be made only on equipment specifically designated by the Director of Security for the reproduction of classified material. The Senate office which reproduces classified material is responsible for immediately bringing all copies under proper accountability controls and notifying the Office of Security of the particulars as provided for a paragraph 4, "Record of Classified Material."

11. *Exemptions.* Those Senate Committees which have custodial control over large amounts of classified material may be exempted from the provisions of Section II of this manual after the Director of Security has certified their policies and procedures for handling classified information fully meet the standards of this manual.

SECTION III. PERSONNEL SECURITY

1. *General.* A security clearance represents formalization of a determination that an individual is authorized access, on a "need-to-know" basis, to a specific level of classified information. Requests for clearance originate with and are validated by Members themselves (in the case of personal staffs), or, in the case of Senate Committee staffs, a determination by Committee or Subcommittee Chairmen and/or Ranking Minority Members, as specified in the Rules of each Committee.

2. *Clearance Standards for Senate Staff.* The criteria for security clearances require that nominees be individuals:

a. of excellent character, discretion, trustworthiness, and loyalty to the United States;

b. who are citizens of the United States.

3. *Investigative Requirements.* To ensure that personnel meet the criteria cited in paragraph 2 above, the following investigative coverage will be accomplished prior to granting a security clearance:

a. *Confidential and Secret.* A clearance for access to Confidential and Secret information shall require:

(1) A National Agency Check. This consists primarily of a check of the records of the Federal Bureau of Investigation, Office of Personnel Management, Immigration and Naturalization Service, and the Defense Central Index of Investigations.

(2) A personal interview either before or as part of the investigative process.

(3) A credit check.

(4) Written inquiries to present and past employers.

(5) Consent for access to financial records.

(6) Consent for further inquiries as may be necessary as a result of any unresolved issues surfaced in the investigation.

b. *Top Secret.* A clearance for access to Top Secret information requires, in addition to the requirements for a Secret clearance, a comprehensive field investigation of the nominee's background.

c. *Special Access Approvals.* Certain types of classified information require special clearances and access approval. These clearances and approvals are granted on a rigidly controlled need-to-konw basis. Requests from Committees or Subcommittees for staff clearances to special access programs will be processed on a case-by-case basis.

4. *Consultants or Contract Personnel.* Consultants or contract personnel must meet security approval criteria consistent with the sensitivity of assigned duties. Depending upon the proposed use of the individuals, specific investigative requirements will be established by the Director of Security at the time the request for security approval is submitted. In all instances, access to classified information will be limited to that needed in the performance of duty, as specified in the security approval. Any proposed change in the utilization of the individual requires submission of a request that a new security approval be granted.

5. *Denials and Terminations of Security Clearances.*

a. *Denial of Security Clearance.* If, after receipt of an investigative report, the Director of Security judges that a clearance should not be granted, the case will be discussed with the Member who requested the clearance. If the Member concurs, a denial is issued. If the Member does not agree with the assessment of the Director of Security, the matter will be reported to the Senate Majority or Minority Leader, depending on the requesting Member's party affiliation.

b. *Termination of Security Clearance.* The Director of Security will terminate staff security clearances of an individual if:

(1) the sponsoring Member requests such termination;

(2) the employee terminates employment with the Senate;

(3) the employee has committed security violation(s) of such severity as to warrant termination of clearances. If the sponsoring Member does not agree with the termination of a staff member's clearance, the matter will be reported to the Senate Majority or Minority Leader, depending on the Member's party affiliation.

6. *Reinvestigation and Revalidation Program.*

a. *Revalidation.* In order to maintain the number of Senate staff having access to classified information at a minimum, the Director of Security will revalidate the need for staff clearances on an annual basis with the sponsoring Member.

b. *Reinvestigation.* For those Senate employees holding security clearances and approvals, a reinvestigation will be conducted at least every five years. The Director of Security shall maintain a control system to insure such reinvestigations on staff members are accomplished.

c. *Requested Reinvestigation.* The Director of Security will also initiate a reinvestigation of a Senate employee at the request of the sponsoring Member.

7. *Secrecy Agreements.* A secrecy agreement must be executed by all Senate employees who are granted security clearances. The agreement will contain provisions that prohibit the signer from divulging or releasing classified information to unauthorized individuals. Where appropriate, the employee will be required to submit to the Executive branch, through the Director of Security, for prepublication review all writings, scripts, or outlines of oral presentations intended for non-Senate publication, which may contain material or information which the employee is pledged not to disclose by the terms of the secrecy agreement.

8. *Security Violations.* All security violations or alleged violations within the Senate will be investigated by the Director of Security. The formal investigation report will include:

a. A finding on whether a probable disclosure for classified information occurred.

b. A written report of those interviewed.

c. A finding as to the person(s) responsible.

d. A statement as to the degree of compromise involved.

e. The security violation history of each person found responsible.

f. Recommendations for remedial action to preclude recurrence of such violation(s).

9. *Penalties for Breaches of Security.* Senate employees who fail to observe security policies and procedures or who are found to be responsible for security violations are subject to the following administrative actions. These penalties are for inadvertent security violations that concern failure to properly secure classified information and do not involve either intent or gross negligence.

a. *First Violation.* Written notice by the Director of Security or the sponsoring Member and warning of possible consequences of further violations.

b. *Second Violation.* Written reprimand by the Director of Security or the sponsoring Member and warning of the possible consequences of subsequent violations.

c. *Third Violation.* Suspension without pay for a period of five days and a written warning from the Director of Security or the sponsoring Member as to the consequences of a fourth violation.

d. *Fourth Violation.* Suspension without pay for ten days and a complete review of the individual's security file by the Director of Security who will provide the sponsoring Member with the recommendation for a more severe penalty, if warranted. Such recommendation may involve a longer period of suspension without pay and/or result in termination of clearances or Senate employment. Where the recommended penalty is termination of clearances or employment, and the sponsoring Member does not agree, the matter will be reported to the Senate Majority or Minority Leader, depending on the Member's party affiliation.

e. *Two-Year Provision.* In the case of a Senate employee who has served two continuous years without a security violation of the nature set forth above, any violations that he or she committed prior to the commencement of the two-year period will be disregarded for purposes of determining whether a violation is the first, second, third, or fourth.

10. *Security Education and Awareness.* The Director of Security has overall responsibility for the security education program. The Director of Security will ensure that before the granting of a security clearance, Senate employees are briefed on the provisions of this manual as well as other pertinent security instructions. The security briefing and indoctrination will, at a minimum, include the following:

a. The employee shall read the espionage laws concerning disclosure of information relating to the national defense. The briefer will ascertain that the individual understands the espi-

onage laws and will clarify and emphasize responsibilities and consequences under the law if the statutes are violated.

b. The employee must attend a security education class prior to initial access and periodically thereafter. A mandatory requirement for the initial security education class will be the requirement for Senate employees to immediately report such contacts as explained in paragraph 14 of section III of this Security Manual.

c. The employee is required, as a condition of holding a security clearance, to sign a Secrecy Agreement with the understanding that termination of employment or such clearance does not relieve the individual of any obligations in the agreement concerning unauthorized disclosures of classified information.

11. *Termination of Security Clearances, Employment, or Extended Leave.* Those Senate employees whose security clearances have been revoked, whose employment has been terminated, or who are taking extended leave for a period of 60 days or more will:

a. Surrender before departure all classified documents or materials over which the Senate has custodial control.

b. Again read and be rebriefed on the espionage laws.

c. Be reminded that the Secrecy Agreement executed upon being granted a security clearance continues to be valid and that termination of employment or clearances does not release the individual from the conditions of the Secrecy Agreement. As a reminder of their continuing obligations, employees will be given a copy of their Secrecy Agreement upon separation.

12. *Security Responsibilities in Personal and Committee Offices.* A high level of security consciousness and good security practice is a basic responsibility of every person holding a security clearance. To achieve and maintain a strong security posture, a Security Manager will be designated for each Member's personal office and in all other Senate offices which receive or store classified information. Under the administrative guidance of the Director of Security, each office security manager will be responsible for the following duties:

a. Providing security advice and guidance to office personnel.

b. Serving as focal points within their offices for security matters.

c. Promoting general security awareness within their offices.

d. Monitoring office procedures for proper control and storage of classified material.

e. When directed by the Director of the Senate Office of Security, conduct an inventory of all Secret and Top Secret, and special access materials held within their office.

f. Retain a record of personnel within their offices who hold security clearances and who travel abroad. This report shall be maintained in a manner to be furnished by the Director of Security.

13. *Foreign Travel.* During foreign travel, Senate personnel are more accessible to foreign intelligence services. To minimize the threat to the individual or to classsified information, the Director of Security will establish procedures to provide for defensive briefings for persons planning private or official travel to designated

foreign countries. All Senate employees who hold clearances will, as a matter of routine, contact the Office of Security to arrange for a defensive briefing. Such will be provided if deemed necessary by the Director of Security. Since any traveler might become involved in an act of terrorism, hijacking, or piracy, guidance on what to expect and how to behave in such situations will also be made available to Members and Senate employees contemplating travel.

14. *Contact Reports.* All Senate personnel shall immediately report any contact with a foreign national of any nationality, either within or outside the scope of the employee's official activities, in which:

a. Illegal or unauthorized access is sought to classified information; or

b. The employee is concerned that he or she may be the target of an attempted exploitation by a foreign entity.

In addition, all cleared Senate personnel shall immediately report any contact, either within or outside the scope of the employee's official activities, with an official or representative of a governmental or commercial entity of the following communist countries: Albania, Bulgaria, Cuba, Czechoslovakia, German Democratic Republic, Hungary, Kampuchea, Laos, Mongolian People's Republic, Nicaragua, North Korea, People's Republic of China, Poland, Romania, Socialist Republic of Vietnam, Soviet Union.

Uncleared Senate personnel are also encouraged to report such contracts. Reports shall be made to the Director of Security who shall advise the FBI of the fact of the contact, unless the sponsoring Member or office security manager determines that the FBI should be informed directly.

Glossary

ACCESS—The ability and opportunity to obtain knowledge of classified information. An individual may be able to obtain classified information by being in a place where such information is kept, provided the security measures in effect do not prevent him from doing so.

AUTHORIZED PERSON—An individual who has established: (1) a need for access to, knowledge of, or possession of classified information, and (2) holds proper clearance to receive classified information. It is the responsibility of the person having control of the classified information to determine that the requester of the information has: (1) a need-to-know the material, and (2) clearance to receive it. (See also "Need-to-Know.")

CLASSIFICATION—The determination that official information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made.

CLASSIFIED INFORMATION—Official information, including foreign classified information, that has been determined, pursuant to statute or executive order, to require protection in the interests of national security.

CLASSIFY—To assign information to one of the three classified categories (Confidential, Secret, or Top Secret) after determination that the information requires protection in the interests of national security.

COMPROMISE—The known or suspected exposure of classified information to an unauthorized person.

CONFIDENTIAL—The designation applied to information or material the unauthorized disclosure of which could reasonably be expected to cause damage to the national security.

COURIER—Any cleared individual who has been authorized in writing to hand-carry classified material. Couriers are of two types: (1) those who carry material in connection with a specific trip and task to be accomplished, and (2) those who carry material as a regular part of their work assignment.

DERIVATIVE CLASSIFICATION—Classification based on or derivied from previous, officially classified material or prescribed in a security classification guide.

DOCUMENT—Any recorded information regardless of its physicial form or characteristics, including, without limitation, written or printed material, data processing disks, cards, and tapes; maps; charts; paintings; drawings; engravings; sketches; working notes and papers; reproductions of such things by any means of process; and sound, voice, or electronic recordings in any form.

FORMERLY RESTRICTED DATA—Data that have been removed from the Restricted Data category upon determination, jointly by the Department of Defense and the Department of Energy, that such data relate primarily to the military use of atomic weapons and that can be adequately safeguarded as classified defense information.

INDUSTRIAL SECURITY—That portion of national security concerned with the protection of classified information in the possession of industrial contractors to the Department of Defense or other user agencies.

MATERIAL—Any document, product, or substance on or in which information may be recorded or embodied.

NEED-TO-KNOW—A determination that a prospective recipient of classified information, in the interests of national security, has a clearance and a requirement for access to, knowledge of, or possession of the classified information in order to perform tasks or services essential to the fulfillment of a classified contract approved by a user agency.

OFFICIAL INFORMATION—Information that is owned by, produced by, or is subject to the control of the United States Government.

ORIGINAL CLASSIFICATION—An initial determination that information requires, in the interests of national security, a specific degree of protection against unauthorized disclosure. Such classification is not based on or derived from any previously classified material.

PUBLIC DISCLOSURE—The passing of information and/or material to any member of the public in any manner.

REPRODUCTION—The term reproduction, as used in this manual, means copying, duplicating, photographing, or otherwise making a facsimile, replica, or counterpart of an original article, regardless of the means used to copy or reproduce.

RESTRICTED DATA—All data (information) covering: (1) the design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but not to include data declassified or removed from Restricted Data category pursuant to the provisions of the Atomic Energy Act of 1954.

SECRET—The designation applied only to information or material the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security.

SENSITIVE COMPARTMENTED INFORMATION—All information and materials requiring special controls indicating restricted handling within present and future intelligence collection programs and their end products. These special controls are formal systems of restricted access established to protect the sensitive aspects of sources and methods and analytical procedures of foreign intelligence programs.

SPECIAL ACCESS PROGRAM—Any program imposing need-to-know or access controls beyond those normally prescribed for access to Confidential, Secret, or Top Secret information.

TOP SECRET—The designation applied only to information or material the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security.

WASTE, CLASSIFIED—Preliminary drafts, carbon sheets, carbon ribbons, stencils, handwritten notes, backing sheets, stenographic notes, worksheets, and similar items containing classified information. Pending destruction, classified waste must be marked and safeguarded according to its classification.

○

64-268 (160)